NP-030135 [IP-030030]

3GPP/IETF Release 6 Workshop Notes

January 27-28, 2003
San Francisco, USA

These notes capture the workshop discussions. The meeting conclusions are documented in IP-030029.

Thanks to all the notes takers: Keith Drage, Dave Oran, Carl Williams, Dean Willis, and Mark Younge. Some minor editoral cleanup by Stephen Hayes.

1 Opening of Meeting
2 Approval of Agenda
3 Meeting Goals and Objectives
4 Review of Release 5 IETF status and issues

See document IP-030010. These notes do not repeat contents that are already in that document.

Presentation (additional remarks):

?? 3GPP Release 5 is now functionally frozen - 3GPP do not add new functionality to this release, but correct bugs only.

?? Identified main areas of collaboration on release 5 - session control; authentication, authorization and subscriber data handling; bearer policy control.

It was reported that last Thursday, the Diameter base and the 3GPP temporary codes documents were passed by IESG, and therefore went in to the RFC editors' queue.

Issues raised in discussion:

?? From liaison statement sent by SIP/SIPPING WG chairs.

1. Obfuscating of headers. Is information now precluded in these fields? Now treated by networks entirely as user-user. Warning on terminal manufacturers not to assume the privacy requirements of user in inserting information into this field. If the user explicitly inserts information in these fields then it will be carried and the network will pass it through.
2. P-CSCF performing identity checks. Is this an issue to a general implementation signing onto a service platform? Will authorization and authentication type headers be stripped out of new dialog requests as a result of this? No.

?? IESG are now expediting particular items through the RFC editor's queue and this will be applied to many/all of the remaining release 5 open issues.

?? IESG would prefer the errata process to be used for changes to the IETF process. 3GPP needs to find a way of referencing those errata.

?? 3GPP version control. It was asked to be discussed here further. Also warned about unwritten rule that it is not possible to change history. Always someone will have implemented the changes and will reject further changes. Referred also to remaining open issues in liaison and what impact this will have in release 5. No further work will be initiated out of 3GPP in terms of 3GPP specific release 5. There may be a better way identified in release 6.
?? Comment that BYE solution may not need to be deployed. Pointed out that BYE mechanism from CSCF is a mandatory part of release 5 in 24.229.
?? It has not been possible to represent streaming class adequately in SDP in the way that 3GPP may correctly map it. Therefore it is not there at release 5. Can this be carried properly in the IETF protocols for 3GPP release 6, in which additional parameters can be transferred, e.g. the diffserv point code or delay, in order to discern properly the real-time QoS? Identified that this was a general problem in IETF and there will be a session later on this (agenda 6.3).

Chairman captured positions at this point.

?? Release 5 is frozen and will not go back and change this with new functionality. Pointed out that that means future extensions have to take account of there being SIP implementations out there that do things in ways that were not resolved by the work on the SIP/SIPPING chairs liaison statement to 3GPP.

5 Overview of Release 6 items that may affect 3GPP

See document IP-030012. These notes do not repeat contents that are already in that document.

Comments from presentation:

?? SA2 have updated the report from which this presentation was developed. Emergency calls have progressed in SA2. SA2 completion of IMS messaging now moved to June.
?? SA2 work on Wireless LAN - problems with progress work on IMS interoperability.
?? DNS and GPRS top level domain. Some interest in maintaining this from 3GPP side. Will be brought up further in agenda item 6.4. No current 3GPP work item.

Conclusions:

?? Identified that the identification of dependencies is important. This identification is tied closely to the progress of the work from requirements. Where requirements have not yet progressed to protocol specifications, then the identification of dependencies will have not yet occurred.
?? Nothing yet for IMS compatibility cleanup. May need to add items to IMS phase 2 work to cover this.
?? What is the impact of liaison from SA1 to OMA on presence and instant messaging? Will this migrate out of 3GPP to OMA? No, as work is too far progressed in 3GPP to move.

6 Requirement and Architectural Issues

6.1 Stack reusability between environments

Notes on Stack Re-usability Presentation (Gonzalo Camarillo)

Summary of presentation: Presentation stresses the IETF method of developing baseline mandatory-to-implement capabilities for a protocol, and two ways that a protocol may be extended: with negotiated extensions (using Require/Supported) or backwards compatible extensions (where the extension can be ignored if it is not understood). The 3GPP requirement for QoS preconditions is negotiated, and will fail calls if preconditions are not met. Sending BYE from a 3GPP intermediary is another problem.

Mankin: 3GPP – please respond.

Drage: 'thin implementation' and 'profile' – is there a distinct? 'profile' is an ISO term (9646), with MUSTs and SHOULDs and so on. How to document in the IETF the role of an extension that is essentially indispensable?

Hayes: 'thin implementation' negotiates capabilities and arrives at a common set, 'profile' assumes a set of extensions and does NOT negotiate down.

Willis: Other 'profiles' have been done of IETF profiles that have ignored MUSTs and SHOULDs in IETF, hence we use 'profile' to mean this pejorative sense.

Oran: I've never seen any standards mechanism that prevents mutually contradictory profiles; therefore profiles are unsafe.

Drage: Protocol design is equally problematic in that regard.

Kempf: IETF standards process includes interoperability testing at the Draft standard iteration of documents – one solution to protocol design problems.

Narten: Does Drage mean that we don't get interoperability from the IETF?

Drage: Profiles will not interoperate if the base protocol doesn't operate.

Camarillo: Let's return to the subject of the presentation, not argue the semantics of 'profile'. You MUST implement the base SIP spec and use the existing negotiation mechanisms.

Mankin: Is RFC2119 language mandatory-to-implement or mandatory-to-use? We'd like to get to 'use', actually. Because we're getting into trouble with stacks lacking these critical features.

Hayes: Let's draw some conclusions.

1) 3GPP implementations SHALL implement all the MUSTs in RFC3261, including those concerning negotiation. This includes preconditions. Any objections? (Drage: Specifications including the MUST have to 'appear' in the 3GPP timeframe – no retroactive MUSTs.

Icaza: MUSTs shouldn't have to be re-iterated in 3GPP standard – this is commonly disregarded today.

Rosenberg: The need to fall back to baseline operation when 420 is received is only SHOULD strength – so RFC3261 does not absolutely require retries when a setup attempt fails because of Require/Supported failure. It would be nice if 3G added some further clarification of how their user agents would react when there is a failure to negotiate an extension.

Hayes: Of course, operator policy may have other requirements – namely that if preconditions or some similar extension is unsupported, then call setup has to fail. We need to allow operators to set their policies in this fashion if they would like.

Rosenberg: I'm fine with that. There's a difference between allowing an operator to make a policy decision, and designing a UA in a way that it will always give up after a preconditions failure.

Drage: SHOULD is hard to interpret for those outside the IETF.

Rosenberg: SHOULD – "you really ought to do this unless you have a good reason to do otherwise". Need some additional language beside a SHOULD that describes the conditions under which you might not want to do it.

Watson: We're already aspiring towards implementing all that is a MUST.

Narten: Neglecting SHOULDs will lead to non-interoperability.

Hannu: Terminals need to implement just one stack. Limit mandatory requirements to what is absolutely necessary for protocol operation. Maybe we should rely on the network, for example, to specify codecs rather than UAs.

Duncan Mills: 3GPP has already begun to lean more towards implementing SHOULDs in the SIP spec. Previous objections were related to radio interface, but compression has eased 3G's pain.

Hayes: Let's capture consensus. 3GPP SHOULD implement the SHOULDs – a good philosophy for all SIP implementations. 3GPP is a very extension-heavy standards body, and should be friendly about it.)

2) 3PPP SHOULD implement the SHOULD, or explain otherwise.

(Mankin: Actually, you SHALL implement the SHOULDs, but may not use them. We get in trouble when we have incomplete stacks.

Hayes: This is the like the road signs: "You MUST obey the warnings". You're turning SHOULDs into MUSTs.

Mankin: Need to distinguish mandatory-to-implement from mandatory-to-use. You SHALL implement and you SHOULD use. Perils are that over time, your usage may shift and you may wish you had the capabilities that you omitted earlier because they are SHOULDs.

Oran: How do you compute the transitive closure of the requirements of all these groups. Are we saying that 3GPP won't downgrade normative strengths of IETF specs, but may upgrade them? What are we really trying to say here? Why restate IETF requirements unless you want to change them?

Hannu: 3GPP respects existing IETF specifications unless it has explicitly overwritten the IETF normative strength in their own doc. 3GPP SHALL 'respect' the SHOULDs in IETF. Don't want to treat SHOULDs like they are SHALLs.

Rosenberg: 2119 needs to be amended to require language associated with a SHOULD that explains when you may not want to meet this requirement.

Narten: Agreed – language in 2119 says you can't drop this just because it's "not critical". If 3GPP wants to upgrade IETF's normative strengths, fine. If they want to downgrade, that is dangerous territory, enters into profiling, and risks non-interoperability.

Rosenberg: It is unclear what SHOULD means to people outside the IETF. Implementer needs to have better guidance about whether or not a SHOULD applies to them.

Hayes: Let me summarize. In terms of specification, there are some SHOULDs we will upgrade; not aware of any cases in which we downgrade a SHOULD. In terms of use, we aren't going to strength SHOULDs in our specs – that's up to the operators. Allison is asking that we urge implementers to implement the SHOULDs… we can't force people to do that, really.

Willis: What does 3GPP want, as opposed to what IETF wants. What I hear in 3GPP is that people hate options – they want one way to do things. Everything not mandatory is forbidden, and vice-versa. This is a reasonable usage of the term 'profile'. There are two ways to implement optional features – either that optional features are present/not present without any compatibility management, or that we use the compatibility management features available in the IETF specifications. Now of course, sometimes the IETF may make mistakes about this.

Mankin: But everyone has to implement the extension management capabilities of SIP, right? Are you saying "code implementations that way" or "configure them that way"?

Willis: Exactly, what's the real difference? 'Configure' is the right way to do it. However, there is resistance to dead code branches that never get exercised in implementations for 3G.

Narten: Don't consciously decide not to implement a SHOULD in a spec. We can't say "this set of SHOULDs, you don't need to both about".

Basavara: IETF today doesn't require that we SHOULD implement SHOULDs.

Hayes: Say you're a vendor developing a SIP product outside the 3GPP. You implement baseline, and may implement some extensions. This is typical. Inside the 3GPP, however, you have some extensions that you MUST implement. I think your situation is exactly the same as that of someone outside the 3GPP community. By strengthening IETF requirements for extensions, would we in fact engender interoperability problems?

Drage: SHOULDs are often misused in the IETF. Synonymous with: if x then y else z. Need more historical information about why SHOULDs have been used within the IETF. We have the right to negate the SHOULD if the applicability of the SHOULD is not clear.

Willis: (introduces svcdisco as an example) – MUST S/MIME requirement for implementation in registrars, SHOULD use, and UAs SHOULD verify. These are tough SHOULDs, right?

Mankin: We better make those MUSTs, or they'll be ignored. Heh.

Drage: I think it could have been much weaker. "If some appropriate security mechanisms exists, use it, else use S/MIME."

Loughney: Meta-comment. Difference between protocol specifications and implementation specifications. We need an implementer's guide – best practices, etc.

Peterson: Let's have a conclusion that relates specifically to extension negotiation.

Watson: Upgrading a SHOULD means that you cannot neglect the case in which UAs do not support that feature.

Drage: Re-iterates earlier point. Describe considerations in which apply in a document, and if it's unclear, then people will ignore the SHOULD.

Hannu: Re-iterates that creating multiple 'stacks' for different operating requirements is too burdensome for mobile UAs. Downgrading should remove requirements and make implementation of mobile UAs simpler.

Oran: SHOULDs are things the implementer should think really hard about it if he decides not to do it that way. Why qualify this at all in the 3GPP specs? If you do, won't the implementers stop thinking then? SHOULDs are supposed to make you think.

Narten: It's one thing to do "this doesn't apply in a 3GPP environment", another to say "you can skip this".

Hayes: If we were only using UDP, what would you have us say about TLS, for example? We can, I think, leave it to the common sense of implementers to figure out when SHOULDs do not apply, rather than mandating it ourselves. Why should 3G do any work?

Drage: Re-iterates earlier point. Appropriate that 3GPP will downgrade normative language that is not applicable to mobile networks, etc.

Hayes: Compromise? We shouldn't downgrade SHOULD. How about if rather, we allow 3G to elaborate on the applicability of a SHOULD, and explain further conditions under which you might not want to implement that behavior.

Willis: Acceptance criteria and implementation testing in the 3G community depend entirely on the 3G standards themselves. IETF is developing protocol specifications. 3G details implementations. Very different roles. 3GPP specifications therefore tend to be much more narrow.

Narten: How detailed are the contractual statements for 3GPP systems? RFC-level? Section-level? Sentence-level?

Hayes: Often clause-by-clause analysis of IETF specs.

Watson: On extensibility, IETF should better define Require/Supported, and perhaps provide some middle-ground like 'desired'.

6.2 3GPP vs. IETF Security models

This session opened with a presentation on 3GPP security model and the current state of IMS security, by Valtteri Niemi, 3GPP security group chair.(IP-030019)

Synopsis:
- what is background along with GSM security model
- release 99 security, network security, SIP security
Principles: move useful 2G security to 3G.
- add countermeasures against real weaknesses in 2G
Main characteristics is 2G

- user authentication + radio interface encryption
- SIM as the security module.

Improvements in 3G:
- auth data and keys sent protected, keys 128 bits, algorithms public, active attacks prevented.
- mutual authentication between terminal and core network. Goes to core network controller, not just base station.
- three parties: home network, serving network, mobile station. Executed whenever serving network decides.
- User trusts home, home trusts serving to handle keying and data securely, serving trusts home for correct keying and for billing
- different auth algorithms permitted on a per-network basis, but default set designed (called Milenage - "based on AES")

Rel 5 security features:
- protect authentication vectors
- GPRS tunneling protocol (uses IPSEC)
- Inter-operator signaling done by security gateways that have pairwise keying.

Have different requirements and mechanisms for access and network domains.
Use RFC3329 for security mechanism agreement.
IDIM = collection of IMS security and data functions
Authentication done at registration (and only during registration).
Therefore, must register before initiating any services.
First hop integrity protection via IPSEC ESP.
Terminal does not have to support PK operations - can use SIM machinery
Alternatives ruled out 1/2
- IKE: required PK operations in terminal, adds round trips if run together with legacy IPSRA, may require PKI for global roaming
- S/MIME: needs PKI...
- TLS - does not work over UDP, lots of TLS connections on proxy expensive, needs PK on terminal, adds roundtrips (but fewer than IKE)

Eric Rescorla: Q: why not elliptic curves? A: too much computation over symmetric keys
Semyon Mizikovsky: why not IKE? A: need public keys, Q: why not preprovisioned secret keys. First hop P-SCSF - has to be in trusted domain. A: yes.
Allison Mankin: let's not take a lot of time revisiting AKA versus IKE. Need instead to take time to look at RC3261 issues

- Media security currently relies on bearer network security
- futures: WLAN interworking, multimedia broadcast/multicast, support for subscriber certificates, presence, etc.

Jon Peterson: Q: say more about subscriber certificates? A: looking into

PKI using "islands" hooked together with AKA. First authenticate with AKA, then deliver certificates securely. Q: x.509 certs? A: yes.
Bernard Aboba: Q: what's the protocol for delivering certs? A: don't know yet - needs work.
Allison Mankin: would be good if you could express requirements to people who understand enrollment so we can get this right.
Niemi: maybe use PIC, EAP, PEAP, etc.
Jari Arkko: need to solve MITM attack on PEAP etc.

Ted Hartley: Q: once you get to home network, if home needs to talk to subscriber in other visiting network, confirm if outbound to other user's terminal is this just the reverse? A: yes. Q: then are there 3 long-lived SAs. What's duration? A: not specified - operators set this.
Mizikovsky: Q: protection by ESP - what's the algorithm specification - no encryption on first hop? A: integrated authentication but not encryption.
Q: show multiple independent SAs with neighbor, so this neighbor has access to all data, right? A: property of this hop-by-hop security.
Rescorla: Q: any two operators have a single SA between them and all calls go over this? A: one SA per security gateway pair.

Second presentation: SIP security model by Jon Peterson, co-chair of SIP and SIMPLE WGs (slides are 3GPP doc 030020).

- SIP security is not easy (first para of RFC3261).
- security for rendezvous protocol for lots of applications
- has a bit of a "love it or leave it" attitude.

Threat model:
- traffic over public internet - attacker can eavesdrop, forge, intercept packets.
- note that traffic on 3G network may interact with public internet
- Primary threats: impersonation, eavesdropping, disruption (DoS)
- also concerned about user privacy and control - user control not compromised by desire of service provider to exercise control.
- need: authentication, confidentiality, integrity, replay protection

Non-assumptions:
- not necessarily service provider control
- low bandwidth (but do have compression)
- managed network

Security recommendations:
- MUST support HTTP digest
- Servers MUST support TLS
- User agents MAY support S/MIME (emerging requirement that registrars MUST support S/MIME. Also SIP-T requires S/MIME
- algorithm requirements are primarily for AES.

Hope that security model matches up with what 3GPP wants to do.
Some things added on:
- security mechanism agreement - negotiation of security options supported by users agents & servers
- facilitates new mechanisms
- AKA for Digest

Advanced identity management.
- traditional From: header populated arbitrarily end-users
- digest auth solves most problems, but not all. Depends on reference integrity (identity of user in domain d is vouched for by element in domain d).
- problems arise when there are complications: e.g. PSTN interworking, SIP networks with multiple intermediaries.

Keith Drage: Q: What you talk about is at IP layer, what about service layer?
A: Service layer could be easier "but money gets in the way".

Approaches to identity management:
- RFC3325 P-headers allows intermediaries with transitive trust
- cryptographic approach - allows intermediates or UAs to add signed block for identity, anyone evaluating identify makes own decision about trust.

SDP and RTP
- need to protect SDP (S/MIME)
- SRTP profile. key management with SDP not converging quickly in IETF. Need to think about transcoding is not end-to-end.

Legal Intercept - IETF does not work on this.

3GPP concerns: interoperability with implementations that use S/MIME and TLS.
- Proxies must support TLS
- proxy servers MUST NOT tamper with message bodies
- Registrar support for S/MIME

end of presentation, now Q&A

Keith Drage: lot of this not precluded by 3GPP, but lots of people being encouraged to use UDP due to post-dial delay considerations. S/MIME on bodies will come down to operator policies rather than 3GPP specifications.
A: concerns about modifying SDP. If part of any 3GPP spec, this in contrary to IETF principles.

Miguel Garcia: used to have modification of SDP for removing codecs, but got rid of it. Still some modification for setting up media policy.

Confident that this is temporary in Rel.5 and will go away in the future - possibly in Rel.6. May still have to read though.

Allison Mankin: not drop any bodies either.

Peterson: almost as bad reading them

Hayes: getting into areas of network policy. Don't yet know so need way of discovering network policies. Doesn't see hop-by-hop model changing. Might be able to relax.

Mankin: need to figure out what really needs to be looked at. Might be ways to make this visible without compromising end-to-end security.

Gonzalo Camarillo: operators want to say what user can and can't do.

Peterson: this could be tricky

Garcia: no way to do this without looking at SDP - skeptical

Rescorla: why does operator care what codec you use?

Mark Watson: roaming model comes in - why not talk directly to your home proxy? 3GPP model allows hooking to policy framework for access to the visiting network and its radio resources. There are business models that need this machinery, if you want to be neutral to business model you need to support this.

Peterson: sometimes models so costly you can't sustain anyway

Watson: might want to charge at a different rate depending on the service, not just the bit rate.

Oran: what about using a video codec to send audio?

Hayes: visiting network might just enforce bandwidth limits, but home network might have service policies.

Rescorla: two kinds of policy enforcement (a)network acting as agent of user - in which case interests aligned, (b)network is trying to enforce price discrimination - in which case interests are not aligned. Experience of IETF is (b) doesn't work in IP world, so no point in trying to support it.

Hayes: Making a value judgment on 3GPP business models?

Watson: In 3GPP network is likely to be successful in enforcement.

James Kempf: authorization for network use and for services are different - might help to keep them separate.

Watson: need to look at if this can be accommodated in IETF/SIP security model.

Ted Hartley: better description of requirement for authorization to IETF might help get a better solution without gatewaying. "The network needs to survive business models". Don't need to change technology when business models change. Also, creating dependencies between application layer and network machinery look like wins short term, but turn into catastrophic losses long term. As things get more complex, these dependencies get harder to maintain. Solution has to admit multiple business models.

Peterson: couple of things to go into:
1. S/MIME assumes use of PKI, lack of replay protection, profligate bandwidth use
- can do some replay protection using timestamps in date headers
- assume a web-like PKI workable - SIP proxy can hold certificate for its hostname, same certs used in web security could be adequate - issue site certs to SIP servers.
- skeptical about end-user PKI - never practically realized for email, getting UA certs problematic. Instead start with self-signed certificates, or shared keys.
- bandwidth usage is justified by valuable properties obtained.

Niemi: many things are useful, but have to have priorities. What about shared secrets - how do you get them?

Peterson: use same kind as you use for AKA

Niemi: not recommending AKA - just shared secrets with S/MIME?

Peterson: still can use AKA machinery.

Niemi: academic exercise for Rel.5

Peterson: sure.

Drage: 3GPP doesn't address end-to-security. Concentrate on mechanisms for user agent talking to home domain.

Peterson: responding to reasons why S/MIME and TLS were not adopted for 3GPP Rel.5 authentication/authorization.

Watson: not a particularly strong requirement to hide information from visiting network that is shared with home network.

Arko: focused on signaling security - need more focus on end-to-end media security

Peterson: end result of good signaling security is what allows media security (via secure key exchange). Also identity management is important.

Jonathan Rosenberg: don't forget about other SIP applications besides voice calls - e.g. presence. Can't solve a lot of these things without end-to-end security. Have to authenticate the party doing SUBSCRIBES.

Arko: agree, but wants more emphasis on media security than we have today.

Hayes: need to partition problem to come to conclusion. For access security, is 3GPP stuff considered deficient by IETF folks? 3GPP uses implicit trust, IETF would prefer explicit relationships. Problem with how doing first hop

Peterson: Fact that ESP used only for authentication, could use for confidentiality too. Aren't there confidentiality needs at access? Can motivate why?

Niemi: UMTS/GPRS is encrypted on access already. Not encrypting allows easier compression

Peterson: nervous about relying on lower layer properties.

Peterson: Philosophy that we should be at higher layer (at least one of them).

Rosenberg: other L2's being considered don't do this right (e.g. WEP on 802.11).

Niemi: yes, can take care of this for Rel 6.

Peterson: endless religious wars in IETF on IPSEC vs. TLS. SIP fell on the TLS side because properties seemed to align with web model. Don't re-open. Would go a long way in IETF if someone would explain in IETF how to use IPSEC with SIP and get the same properties.

Niemi: see 3GPP doc 33-203.

Hayes: talked about access - seems to be where divergence in models. In

3gpp there's an implicit transitive trust model. Maybe need to negotiate which model is being used.

Rosenberg: seems like you're trying to address this in Rel.6. Proxy-to-proxy security is very important. TLS needs to be available at MUST strength for inter-proxy security

Hayes: it's a MUST so it will be there.

Mankin: shown how easy it is to become a carrier and then become a peer

Hayes: also need bilateral roaming agreements.

Rescorla: what happens when somebody breaks into Verizon and steals all their keys?

Hartley: might want to re-key after some number of packets. Trying to get at the implications of long-lived SAs in transitive trust environment with not other protections.

Hayes: Rel.6 addressing network to network key distribution - working on PKI for this

Peterson: somewhat uncomfortable with IPSEC security gateways. Assumes a lot about security of the ingress. Prefers TLS or even IPSEC on SIP proxies.

Watson: there's IPSEC from proxy to security gateway as well as between security gateways, but former is optional.

Rosenberg: time has shown that topology changes and what was once secure is no longer secure.

Peterson: important to have end-to-end security, e.g. for identity. Crypto approach allows an signed assertion of identity - finer granularity of trust. Once you get into things like SAML, you really need to know who is asserting something.

Watson: in principle this is fine - there's a lot to the inter-operator trust relationships. Just by removing the identity piece you still have other stuff.

Mankin: not saying the end-to-end is complete replacement for hop-by-hop, right?

Watson: end-to-end doesn't do everything needed to set up trust relationships with operators.

Drage: implementation in P-asserted-identity is very integral, so replacing it with cryptographic identity is not likely to happen in Rel.6.

Hayes: Might be willing to overlay end-to-end for cases where it can substitute for hop-by-hop stuff. But need a way of know this dynamically.

Niemi: TLS is hop-by-hop.

Peterson: yes, but for example registration in IETF basic SIP is one TLS hop to the home registrar.

Rosenberg: look at presence and IM as driver for looking at additional mechanisms in Rel.6. What do operators think users want/need here?

Hayes: any objections to Jonathan's approach...seems not. Let's get operator feedback.

Mauricio Arango: Seems IETF prefers a model where there are only two proxies. Why?

Peterson: can get reference integrity if upstream proxy is in same domain as the initiator, and downstream proxy in same domain as target.

Arango: assumption that proxy has not been compromised?

Peterson: yes.

----------break occurred here----------

Went on to some proposed conclusions
- 3GPP & IETF should collaborate on requirements, threats and protocol for enrollment of user certificates. Allison and Steven will figure out which parts of IETF and 3GPP should get together on this

- 3GPP should adopt a goal of graceful security interoperation with the RFC 3261 features (S/MIME, TLS)
Drage: nothing in 3GPP that stops this today

Garcia: not a problem

Drage: all the MUSTs/SHOULDs in 3261 are intact

- 3GPP and IETF will try to understand together the various service authorization requirements at the application level.

Hartley: complicated. sometimes operators want to police, sometimes control QoS. Expose info to operators. Useful to know what the set of requirements are. Especially to do this in such a way as to not require constrained network topologies.

- hop-by-hop architecture: IETF comfort level with access security and edge-to-edge models in particular:
- IETF identified issues with there being no spec for operational issues on key management (time, revocations, etc.)

Hayes: much of this is operational and in the domain of deployment, hence not for 3GPP.

- IETF would prefer TLS between proxies, or at least mandatory IPSEC between proxies and security gateways (still open)

Hannu Hietalahti: a bit nervous about making this mandatory for deployment

Hayes: operator can decide to not have a roaming agreement with a partner not deemed sufficiently secure.

- 3GPP will use presence and IM as a driver for enhancing the 3GPP security model.

6.3 Network vs. User Control

Three speakers presented during this section. The speaker names and presentation titles are:

Jonathan Rosenberg, Dynamicsoft
Proxy Assertion of Session Policy an IETF Perspective (IP-030021)

Martin Harris, Orange Innovation
Network Control vs. User Control (IP-030003)

Alex Harmand, O2
Network versus User Control: An operator view of user service (IP-030007)

6.3.1 Talk by Jonathan Rosenberg

Jonathan Rosenberg is Chief Scientist at Dynamicsoft and involved in much of the SIP specifications within IETF. Jonathan is lead editor of the SIP specification itself (RFC 3261) and also other specifications such as SIP Presence and Instant Messaging. Jonathan is also co-chair of the IETF IP Telephony working group (iptel).

Jonathan talked a little bit about "Proxy Assertion of Session Policy" and what "his" IETF perspective of what that means. Session policies are things that affect the media sessions themselves such as if they flow through intermediaries or what types of codec are used or various parameters that deal with the media. We are talking about a condition here where a proxy is interested in saying something about how those sessions should work. In the very beginning when RFC 2533 came out proxies just didn't do that. The role of a proxy server was routing signaling services and had nothing to do with sessions and their parameters. This was an end to end problem – there was no reason that the proxy would care about that. That so obvious – ASP model – total separation between the provider of the SIP capabilities and the access and IP network provider. There is no reason why the SIP providers should care about what the IP network looks like. So we didn't care about this problem.

Needless to say through various applications of SIP - experience shows in cases where they are not separated (where in fact the IP access provider and SIP application provider are the same such as 3GPP) there is a need for the network to say something about the session policies. SIP is used to set them up is a natural means to do that. This came up as particularly important in two cases:

- NAT and firewall traversal

  Ex1: The midcom group within the IETF has specified how a proxy can control a firewall or NAT and if controlling a NAT means obtaining IP addresses it will need to modify SDP in order to reflect the new addresses it obtained from the NAT.

  Ex2: More general having media close intermediaries that the proxy might know about is one way of solve some of the NAT traversal problems.

- Codec grooming

  Came up particularly in the context of 3GPP. Understood from IETF side that it was a requirement that the network operator be able to say "no you can not use G.711" or "no you can not use video right now" - so it might even be a time of day thing or dynamic based on network congestion ... Have to be a way for the operator to say something about the codecs that you use.

To date, this has been accomplished through SDP editing, a process where proxies dig into the bodies of SIP messages, and modify them in order to impose their policies. For example the proxy would see SDP coming by and see a codec in there it didn't like and it would change the SDP. However, Jonathan states that SIP editing technique have many drawbacks:

- Fails with e2e encryption: proxy can't look at SDP to say what's going on. Simply CAN'T do it!

- In case of just integrity protection (no encryption but just authentication and integrity check) proxy can look at it but can't change it because it will cause authentication checks to fail.
- Requires proxies to know SDP and its extensions – a drawback. Becomes a bigger problem when you start to worry about transition to new sessions description mechanisms like SDPng.
- Proxies have to pay attention to things like Require.

  A UA may require that an extension be applied to the SDP body. This is accomplished by including a Require header in the SIP message. Proxies do not look at such headers. If the proxy processes the SDP without understanding the extension, it may improperly modify the SDP, resulting in a call failure.
- Jonathan says this introduces new "points of failures".
- Scalability problems - One of the reasons SIP scales so well is that proxies don't have to be aware of the details of the sessions being established through them. If a proxy needs to examine and/or manipulate session descriptions, this could require many additional processing steps.
- CONSENT - Ultimately, end users need to be in control of the media they send. If a user makes a call through a SIP network, they have the expectation that their media is delivered to the recipient. By having proxies modify the SDP in some way, they act in ways outside of expected behavior of the system.

Jonathan proceeded to speak more on "Consent". Robust networks are based on a contract between client and network. Client sends a type of message asking the network to do something. With expectations it does what it is asked and sends a failure if it can't do it. It doesn't do unexpected things that go beyond the bounds of its contract. So the network does what it is asked – no more and no less – in general definition of what is being asked. Contract violations where the network is supposed to do things that are rather unexpected ultimately lead to very bizarre application failures.

?? Example is NATs: IP service contract is very simple - you send an IP packet to an IP address and gets received there and the IP routers don't look at the contents of the IP packet. Based on that contract you can build all sorts of applications that do all kinds of things which you can make those assumptions. You can probable assume that the network is not violating this contract of IP service. As soon as you put NATs in there they violate that – they do all kinds of horrible things. Jonathan told us that recently he heard of some new horrors: a whole class of NATs that look for textually and/or binary encoding addresses in a ***payload!*** Whenever they see them the dirty NATs will rewrite them based on the NAT operation. "of course this is going to help:-)" can't tell us how many horrible things it does...

?? SDP rewrite: one of the things that happen when these failures occur is that they are mysterious. User didn't expect it to happen when it made the call but it did. What happens if an error occurs – there is no way to trace easily or for the end user to know what kind of problems or for the device to react in a reasonable way to a failure because it was so mysterious. My email fails because some NAT in middle of

network decides to rewrite the IP address in middle of packet – how does customer support handle the call.

?? We don't want the network to interpret user intent. That is really what is happening with these codec grooming techniques. How do you know that the user thinks it is ok to get rid of video or get rid of a particular codec?

So to deal with some of these problems the final 3GPP spec has a solution using 488. Idea here is that client sends INVITE with SDP – network rejects with 488 and provides allowed codecs and media types. Benefit is that user knows what has happened. It is sort of a bridge for failure. Drawbacks: There are many: (1) increases call setup time because we get these down signal messages (rejects, try again) and gets worst the more number of hops try to do this. (2) only useful for codec and media stream grooming – doesn't help NAT. (3) user still doesn't know that it is the network that has the constraints – client can't tell that the network rejected the request because of the problem. (4) still doesn't work with e2e encryption – but works with authentication. We need a better solution than this.

Jonathan has been working on requirements for the ideal solution. These are captured in an IETF internet draft:

Requirements for Session Policy for the Session Initiation Protocol (SIP)

http://www.jdrosen.net/papers/draft-rosenberg-sipping-session-policy-req-00.html

Jonathan then proceeded to go over these requirements for the ideal solution.
Please see slide presentation (IP-030021 workshop document) and/or draft above for full enumeration of requirements. Listed below are a few examples:

- Policies can be per-media stream and in each direction. For example, maybe possible to prohibit someone from sending G.711 but ok for them to receive it. It should be possible to impose this kind of policy.

- Should allow insertion of media intermediaries. General ideal is that anything having to do with the session that is interesting the proxies ought to be able to say about it. Jonathan proceeded to comment on one point here: QoS reservation where it provides QoS parameters – request for the network to please use this diffserv TOS parameter – this is in scope of these requirements.

- Source routing ability - in case of media intermediaries – want to traverse. How that happens today is that we don't know that there is an intermediary. When I call you the IP address I see is actually of the intermediary. I send media there and it happens to have a dynamically constructed mapping table that then forwards the media to you. So that creates this route between me and you by storing state in the network that describes that route. Alternative approach is source routing: where I am told explicitly please send me in through that intermediary and from that intermediary from me to you. And if I had a way to specify that source route in the media path,

the state for it now gets pushed to the end device. And I can see what happens so there are some consent benefits. Useless for RTP. IP-IP encapsulation is better but overhead associated with that for RTP is too significant for RTP. There are other things instant message sessions that don't have those problems – for those kind of things – source routing would be helpful.

Intent of this is develop a new mechanism that allows for proxies to impose a request session policy that meets the 3GPP requirements but also meets that the requirements that IETF is concerned about such as "CONSENT" and improving failure mode cases. One of the things that Jonathan is very concerned about is network derivation of user intent. That is the essence of the problem. There is SDP data that is meant to describe an end-to-end session and the network derives some kind of interpretation of what it means or why it is there. The user didn't intend the network to do this – the point of this SDP data was NOT for the network to do something – it was for the other side to setup a session. When you try to infer user intent with end-to-end user data, you introduce potentially bizarre failure modes. All kinds of problems with misinterpretation that we try to avoid.

Essence of requirements: it is not basing decision on what is happening based on end-to-end data. This requirement means that the solution must have additional data explicitly meant for the network to use to assist in imposition of session policy. For example, client can say to the network that this stream is a conversational stream and this stream is a streaming video. And based on that explicit declaration by the end user the network can do something. So it is one of general thing that the user can tell the network that the network can then make some decision about (i.e., what codec I am using, where I am going). Don't want the network to derive decisions based on assumptions.

Comments on mapping: Not addressing mapping issue. Addressing interpretation of what the user wants and changing role of the message as it goes through. There will always be a mapping and that is sort of different issue. Hayes sees a need to address that but anytime you have SDP you have to map it into some sort of bearers or services and that is separate issue than what is being addressed here.

Jonathan proceeded to discuss "CONSENT" requirements.
Why do we have CONSENT requirements? (1) to eliminate some of these bizarre failure cases. (2) make sure if the network imposes a policy the user is happy with the call proceeding with that policy intact. It maybe that if the network says unless you get rid of that codec you can't make the call. That's ok. I am ok with allowing a 3GPP operator to say that but I like for it to be possible the end device (end user) to know that is why there call failed. See slide presentation for CONSENT requirements. Below is an elaboration on one of those:

- Proxies can inform UAC/UAS of implications of non-compliance. For example, in case of intermediary it is useful for an end point to know that their media stream is going to close their intermediary. If they choose not to use that intermediary and try to connect directly, the implication is that you won't hear the media because we have a firewall that blocks anything unless you go through that intermediary. So that is the implication the

UAC or UAS may like to know about in order for it to make a decision on accepting or rejecting policy.
Jonathan discussed security requirements. See slides and requirements draft for enumeration. One key requirement that Jonathan elaborated on is provided:

- UAs can verify the identities of proxies who made policy requests. So as soon as we get players who that say something about what is happening in a session you liked to authenticate who those players are. Don't want to be able to have some help in the middle of the network and modify my SDP and ask me to do something without knowing who they are. So for example, if the network says please don't use G.711, I would like to really know that they "really" said don't use G.711 as opposed to something else.

Jonathan described a proposed information flow on how one might accomplish this. He provided a diagram with user agents with two proxies. See presentation slide for this information flow diagram. This diagram illustrates straw-man proposal of explicitly defining what network usage of those policies with user consent. Get out of pit of having network interpret things. The explicit purpose of this information is for network to impose policies on it. It has been designed for that purpose.

Allison: Focus on requirements. People shouldn't think that this is a proposal.
Jonathan: View of how these requirements may work. Useful of how to do this. Not an accepted work item of SIP group. Jonathan has written an internet draft (it has since expired but is on his personal web site). Jonathan noted that this is just an example to ground in reality.

Important thing is what are requirements. What are the 3GPP requirements. Do these things make sense and this is what Jonathan would like to discuss.

Two drafts: Requirements draft listed earlier. Second draft detailing the information flow is at:

Supporting Intermediary Session Policies in SIP

http://www.jdrosen.net/papers/draft-rosenberg-sipping-session-policy-00.txt

Hayes: Good description of a general mechanism to solve sipping problems for SDP manipulation. Important to understand what types of things we may need to modify. Need a generalized solution to meet all of our requirements.

Comment: backward requirements. List some fallback to generic behavior.

Operators from Orange and O2 operators will provide requirement inputs...

6.3.2 Talk by Martin Harris

Martin Harris of Orange Innovation gave a presentation on "Network Control Vs. User Control". The document number is IP-030003. The talk was focused on operator requirements.

Martin says the presentation goes into what Orange sees as its business model as a mobile operator. Things that are seen as key as a mobile operator – Martin says revenues are obtain via access, services and content. Objective is to increase the customer base and average revenue per user. Facilitate this by the protection of the network and users from fraudulent use. It is important for them to assure their revenue. They have an on-going relationship with their customers via the subscription that take out with them. They are the point of call in the event of the many problems – need to provide a quality network in order to keep their customers and increase their revenue. Something that is unique to mobile operators is the requirement to ensure spectrum efficiency. Mobile operators provide networks over radio spectrum – it is a finite, shared resource that is very expensive. For example, UK operators pay 6 billions dollars each for 10MHz of 3G spectrum. It is combined with high cost of deploying new access technology and new base stations. Martin says that what we need to do to maximize spectrum usage and service capability to ensure that we can get better usage for that spectrum because we are not going to go out and buy more.

Martin looked at the three points individually:

- Protection against fraudulent use – make sure that the operators are paid for what they provide. See new world of 3G technology is IP. For many people they see that the Internet is free - not quite true as we provide for the access but IP based mobile communications will not be free. That is a great concern to some of us that will be an incentive for users to hack into mobile communications and try to get a better service that they are paying for. Various charging models will exist on the Internet. This includes different charging models for different accesses. Another major charging model deals with QoS. QoS has been mentioned many times as potential distinguishing factor that mobile operators have to offer to their users (i.e., real time vs non-real time and gold, silver, and bronze service). Martin states that if you ask mobile operators how they will charge for services in 3-4 years from now they will answer that "they don't know". Martin states that what they want is the flexibility and capability to be able to adapt the charging model to the environment as it stands in the future depending on what the customers want. Mobile operators are also looking to charge based on content – not charge based on access technology or quality of service but purely on content that the user downloads. Operators needs to be able to exercise control in order

    - to authenticate the user and authorize their access
    - accurately account for (and charge for) what resources are being used

- prevent the users from obtaining something for nothing

- Quality – give the customer what he wants and meeting the customer requirements. Wireless networks should provide a service that is better than the service that networks today provide. That is a big challenge for mobile operators – we have to accept that within the access network there is a long round trip delay (typically 500ms). Martin states that this is a delay that we have to live with so if we are looking at a call setup that sends additional messages back to the terminal – back to the network – back to the terminal – back to the terminal – we are looking at 500ms additional delay each time. That is not going to give us a service better than circuit-switch. James Kempf commented that most of that delay is in RAN and Martin agreed. Martin is not asking IETF to minimize or reduce – it is something we have to live with. James Kempf says that why doesn't someone talk to RAN working group 3 and fix the problem in the access network. Martin states that there are fundamental issues that they have not been able to overcome. Martin wants to provide a high-level of reliability; thus, we need to provide inter-operation (i.e., response to 488 messages). Ensure that if a terminal does respond – that it does so correctly and efficiently. Martin states that their are some of us that don't trust terminals – don't know what users will do to terminals and what type of applications that they will download to the terminal. For example, if a customer downloads a bad user agent into terminal and it misbehaves the customer will call the operator. It will be there fault. Martin states that another requirement is to provide a range of interactive services to the users. Customers will have expectations of high quality from mobile operators – customer care is high cost for operators. Martin states that operators want to make sure calls and sessions are setup efficiently and quickly to give the customers what they want. So mobile operators want to exercise control in order to provide fast session establishment in line with user subscription; renegotiate bearer to suit environment and application; and clear down and clean up sessions in the event of loss of connection.

- Maximize Spectrum Capacity : don't want to waste this limited resource. This will reduce the capacity for users and data rates and reduces coverage. As a result, this will reduce the potential for revenue and it will also increase mobile operator costs. So from the signaling perspective mobile operators don't want to see unnecessary data transported over the air interface. No unnecessary signaling over the air interface. No unnecessary usage of bandwidth. No unnecessary error detection/correction. Martin states that we should use data compression techniques where practical. In Summary, Martin stated that operators need to exercise control in order to ensure terminals, applications and users do not abuse air interface (the one that mobile operators paid for).

This comes down to user versus network control....

End-to-end versus end-to-middle-to-end. Martin stated that he calls it a man to middle model but that means something else within IETF. Traditional Internet model is really end-to-end where the intelligence is in the terminals. But if you want services – how are they handled when the far end is off line. Users will mix-match a wide range of

applications on their terminals. Users will get frequent crashes and lack of interoperability. Martin queries: "Does the ISP fix this"? Martin doesn't think so... Martin explains that the main "Mobile Model" provides a wide range of easy to use services customized to the type of terminal that the user has and the bandwidth that is available. We see that we manage session establishment – efficient and transparent establishment of the core to the far end – and we support the user in the event of any problems.

So to summarize: operators need to be able to exercise control on the network in order to protect revenue, provide quality, and ensure efficient spectrum usage.

James Kempf commented misunderstanding here – OPUS draft that describes the roles for intermediaries – intermediaries can't be transparent to the party that is acting on their behalf. What is not good is for any flow to go through the intermediary to be arbitrarily being taken apart and rearrange by the intermediary when the end didn't have a say about this. Should look at the RFC as it provides guidelines on providing this kind of service.

Someone commented that we shouldn't challenge the business model of the operator but with the technical implementation of the business model. Sometimes we are skinning the cat the wrong way so let's keep this in mind as we work through this. Find a good technical realization that enables the business model.

Hayes: requirement to have network controls imposed in a reasonable way.

Someone commented that IETF stresses end-to-end model at transport layer not the application layer. One example is with SIP – uses proxies.

Jon Peterson: As you progressed in your presentation and way you talked about intermediaries and be available when users are off-line and so forth – doesn't violate what he understands to be the end-to-end model. In fact Jon believes the end-to-end model to be totally compatible with the ideal that there is some entity that's on-line, for example, with something you register with that if you are off-line send a request that this guy is off-line ... Hayes said so that your end-to-end doesn't necessarily mean terminal to terminal.

6.3.3 Talk by Alex Harmand

Alex presented a talk on "An Operator view of User Service".

Alex discussed mobile services. Circuit-switched services in which voice and data over circuit connection. Packet switched services of IP via GPRS network; cellular enhanced IP network and allows end users to run IP applications. All via common radio network (GSM 900, 1800, 1900, W-CDMA, etc). Other mobile service to provide Internet connectivity and PSTN/ISDN while on move. Provide for QoS, customer support and variable charging and tariffs (i.e., volume and duration, bundled and free minutes).

Coverage for mobile service deals with radio base site provision "squeeze the limited spectrum".

Alex proceeded to discuss mobile network connectivity with SIP. Alex noted that network can enhance connectivity. For example, taking care of radio capacity. There are a lot of methods available such as optimized codecs; we can use transcoding as well; header and SIP compression – all which will reduce costs for user and network and improve quality. We believe that the network can play an important role in roaming with legacy mobile networks – useful when user moves outside 3G radio coverage.

Alex noted several architecture aspects for mobile connectivity. Thanks to work with IETF and 3GPP we are re-using IP transmission over wide cellular coverage area. Here we adopt IETF SIP signaling methods for wider spread IP connectivity of services and users. 3GPP is based on several session servers (P-CSCF, S-CSCF ...) - link of SIP session and underlying bearer ---- opportunity to add application server.

With user to user – user can run end-to-end via raw IP if required ---- directly over GPRS (IP) network bearer for 3GPP cellular. Connectivity at IP address level. Will require additional (network) support if wider connectivity is required.

Alex provided summary that key success for mobile services are: (1) ease of use; (2) connectivity; (3) QoS; (4) Flexible service package. SIP enhances basic mobile services in that it provides a rich call over IP and presence and messaging.

6.3.4 Comments/questions/discussion on presentations...

Comment: Why would you have the application server within the 3GPP network as opposed to outside of it. Also, from mobile operator point of view- it can be possible to provide mobile service based on non-3GPP compliant SIP server without governing IMS based services regarding compatibility (??).

Keith: 24229 says application server then it should follow 24229.

Hayes: Frame some questions...

Operators would like a fairly efficient mechanism to charge for different aspects of service – they don't know exactly what that means now. To charge we must have a way of policing different aspects. Hayes asks if anybody does agree with that assertion "that we need to be able to efficiently policing different aspects of SIP services".

Dean Willis (DynamicSoft): Kind of disagree with it. Because it implies a solution in the way you frame the problem. Yes, we absolutely need to be able to effectively allocate and manage the resources to meet the business models put forth on slides. Problem is as I stated it comes down to the technical implementation of the realization of that. The construction that we put forward in 3GPP provides a mechanism for controlling bandwidth of those things that were negotiated with SIP. It doesn't give us any way to

broker services, to control bandwidth and do QoS with those things that were not negotiated with SIP. As much as Dean likes SIP – it is not the whole world. So we put artificial barrier on the opportunities for operators to generate cash out of their network by putting this constraint in the design model.

Dave Oran (Cisco): Experience that some of IETF people would note is that people would tend to police the cross product of the network layer, the transport service and the application service carrying bits are where a lot complexity failure proneness and wall gardens show up. I don't think anyone in room would object to "we need a way to police what users do in terms of how much network bandwidth they use, how they operate over the airwave, and what type of QoS they get. I think similarly no one is objecting in saying well that an operator that is operating an application service needs a way to police which of those capabilities, what transactions a user can do, what data he can see or not see, and any of those disadvantages of those applications. But where I think we get off the boat is when we say that we want to police the combination of those things as one element – because that binds the application to the usage of the network in a way that history has shown only works for a very short period of time until people figure out a way to defeat it.

Comment in response: I get the point there that it is more complex if you want to police that combination and that matrix there. The question remains the answer to whether that complexity is justified with the additional revenue 3GPP can make. That doesn't mean we shouldn't satisfy how it would be done if it needs to be done – because of the fact of the matter is that governments around the world are asking 3G operators to be tax collectors and there is a lot of money that has gone to the governments and that has to be repeated (??) in some way. And people have judged so far that you need these mechanisms – you need to be able to charge based on services in order to get the revenues that justify the continuation of the industry.

Dave Oran (Cisco): If it is so complicated, why are operators always doing it that way. I believe it is to exclude competition mostly – there is no technical basis for it.

James Kempf: The reason it is done this way is because it is the way they have always done it. For example, if you look at SS7 like IS41 – it's got everything in it – its got mobility management, its got DIAMETER… etc…

Ted Hardley: Point by Mark need to stress… IETF is not trying to tell 3GPP that everything has to be "bit transport". What we are trying to sell is that you will probable get the widest range of potential services by having the most open architecture. Ted said that he and Allison Mankin were talking about this at break for a moment – if you put a control break at every possible place in the network, it is expensive and now you have to have that much more state in the network to manage that all those control points to deliver a particular service. What we are suggesting is to look at architecture that allows you to over these services without keeping that much state in the network. And maybe that means we end up with something like you have now where there is a single point of access where the state is maintained. Maybe you end up with something where that

point can be in different places of network topology. We are not trying to say "don't offer services above raw transport". We are trying to say the most open architecture will give you the widest range of essential services. That is good news rather than bad news.

Hayes: What we heard from Martin is that we won't be able to do openly is charge for content. Content can be defined in a lot of different ways. Since the operators don't know necessarily yet how they are going to define content, so it is not just being able to provide services in a wide variety of ways but it is also being able to differentiate between the services and charge for them in different ways based on different types of dividing up of what the user is getting.

Ted Hardley: Makes my point better than I did…. If you don't know what you are going to be charging for, an open architecture will give you much more flexibility to charge for different things. Once that you know that I am going to be charging you for 56kps voice circuit from now until the end of my monopoly. I think the point that you just made is really important for the IETF to understand about your problem – you need to be able to offer different services over this network and there are billing components to that that we need to understand. The fundamental thing here is that we really believe (our IETF bias) that more open your architecture the more services you will be able to offer – and ultimately the more $$$ you will make. **It doesn't become raw bit transport because you made it an open architecture.**

Hayes: I don't think we are really approaching a closed architecture – but we don't want from a protocol point of view that we restrict things.

Comment: Operators are trying to move toward an open architecture – this is what OMA (Open Mobility Alliance) is trying to do through web services interfaces. An area that OMA is not addressing is session control. It is important to keep in mind that location information, presence information, messaging functionality. People in OMA are working to provide web service based access through this kind of network functionality in a pretty much end-to-end approach – so this is important to keep in mind as a priority.

Thomas Narten: Alarm bell that raises for me is pre-mature optimization – where this intense focus on "we've got to minimize protocol overhead – that we've got to do this – and leaves us with a solution that is really scoped around trying to minimize a round trip or eliminate a round trip or minimize the bits on this link. This is shortsighted. The community is very sensitive and open to idea that we want to minimize bandwidth – we don't want to waste it. But it is note the only thing that we consider that is valid. What our architecture likes to do is to be an enabler for new services including for services we don't understand or have yet to be invented yet. So we talk about what to do with charge for services and so forth – Thomas says this is fine – but he states what is not so fine is when you are initiating a very narrow set of services and that is what the architecture is focused on and the other stuff that hasn't been invented yet or you don't think that your going to make $$$ off of right away is that is something is sort of included and fixed in and later becomes a barrier to actually deploy that kind of stuff. If you have an open

architecture that allows for future development, 3-4 years down the road someone can ease it in without having to re-architect. That's a win-win….

Hayes: That is what we want. Want open way so that we can have informed User agents so that we can make intelligent requests of the network. As far as the actual enforcement that can occur at the CSCF – don't really trust the User agents. So we've seen a set of requirements from Jonathan to send no additional roundtrips, etc… What we do in 3GPP we need to access those requirements and make sure those requirements give the platform for having the necessary network control – platform that we can use for making intelligent choices in the EU. 2nd thing: what types of policies we actually envision – more than using codecs and bandwidth. What we need to get a handle on is what type of things we see – how many different ways there are to cut this pie – in future we know a lot of those turn out that are never used. I think if we can understand some of the different ways that we could potentially charge and determine what the different criteria are – then we can provide feedback and then we can drive a decision on what type of policy information collection mechanisms maybe needed.

Dean Willis: Never been able to express ways 3GPP are doing some things. Problem in way we decided to provide for the business model of differential charging for things – three things in network that have fees associated with them. The way we are doing this in 3GPP right now is that we are sorted of guessing the things I am talking to and then have the network equipment meter it off appropriately and charging me differentially for the bits I am using to get to that thing. Metering bits differently depending on the application. Problem is that this creates an incentive for me (the hacker) to find a way to fool the network. Way that I want to respond to this – is that instead of metering the network bandwidth to a particular thing – monitor the usage of that thing and track network utilization and then later put together the billing to figure what I really owe.

Jonathan: This is here nor there… This particular debate point is not a new one. What I thought the point that this session was to focus the feature we want to provide is the ability of the network operator to impose policy on the session and how to go about doing that in a reasonable way. Rather than say you silly 3GPP operators, you can't impose policy on the session. Jonathan contends the reason you may want to impose policy on session may be for the benefit for the user.

Dean: What is a reasonable way to impose policy here…

Jonathan: We want requirements for what a reasonable way of providing policy. Those are requirements essentially.

6.3.5 Few conclusions presented by Allison Mankin from previous day:

- The intermediaries should have ability to express and impose control, with a careful architecture. IETF will develop requirements for generalized solutions beyond 488. The initial text for 3GPP to review against operator needs is draft-rosenberg-sipping-

session-policy-req-00.txt. 3GPP will study these requirements. IETF will on directions in this area. RFC 3238 (OPUS) provides an architectural perspective overall.

- The longevity of the policies, how they will change from one session request to another, e.g. how dynamic they will be are questions that may affect the nature of the work we have described. This is referred to the requirements development in 3GPP.

Allison states we are pretty far from potential mechanisms. Hayes states that what we get from this workshop is a commitment from 3GPP community is that they will review the requirements and look at what intermediaries implementing control is needed. And IETF will look at a general solution that will meet the requirements.

General comments were made on how to get work done within 3GPP groups and to proceed within IETF.

6.3.6 Remaining issue: Bye

P-CSCF sends a bye on behalf of the terminal of the terminal goes out of coverage. [not coming from trusted party]. Informs party that the connection is terminated. We are doing network BYE – problem with BYE in that it is not coming from a trusted party. It may be ignored by UE doing integrity detection. Like to open for discussion and how to resolve the issue.

Comment: From Miguel requirements draft – where that requirement is inadequate. Section 6.14 of draft deals with problem of phone dies or administrative disconnection. Must release network resources, stop billing. 3GPP proxy sends BYE is preferred by 3GPP. 3GPP requirements to SIP internet-draft is draft-garcia-sipping-3gpp-reqs-*.txt. Please see section 6.14 for requirement that is being discussed here at the IETF-3GPP workshop.

Comment: Wanted to know time-frame that you need to release this state.

Mark : If person going out of coverage and still paying for the other parties access charges. Don't word requirement in terms of a particular solution. Only mechanisms is "event framework". Didn't consider "event framework" for this problem because they considered what that would entail. 8 subscriptions for every call… anyway it's a lot of subscriptions…

Jonathan: It all depends on who needs to know and why and what kind of time scales and what the trust relationships are between various things. One model that works in some cases for that call over the end points that were described to you – notification service – notification is lost at one of the ends – you know longer continue with this call because you ran out of resources – and BTW sending a BYE is not sufficient; there is the assumption that there is some kind of coupling of that to turn off connectivity at the IP media transport layer. You can argue that really that the only important customer of the notification artifact P-CSCF from a billing perspective - for everyone else it is a cleanup

or an informational perspective which has smaller time tables and maybe it is ok to rely on endpoints sending a BYE (??). Jonathan notes it is not entirely clear to him that it is 8 subscriptions for every call…. It may be somewhere between 2 and 8 depending on working out the details of how the mechanism operates. But the clear benefit if we put this in the event framework then it is the endpoints that send the BYE. It requires some more thought.

Dean: Requirement is for the system to somehow to respond to the loss of access appropriately. Don't know which entities in network are able to detect loss of coverage and where we can effectively enforce that operation at the other end. IETF perspective billing directly off of SIP signaling is a bad ideal -- there are other enforcement points that can be brought into this.

John Peterson: We've been studying on this problem for a while – John's view is that this is not a SIP problem as such. Doing action at bearer level is totally sufficient for this.

Miguel: Clarify – operators want to use time base charging. If this case, need an accurate mechanism to inform entities that are accruing charging.

Jonathan: No one disagrees with that. Point to be made: only accurate way to meter for time duration of calls is not at SIP level it is bearer level. They account for what they do and you bill for what you account. Time duration for session lives in session bearer count. You have elements that know that – you've got things that know that.

Comment: Consider other case where if you go out of coverage you need to stop at other end call accurately. So you need some sort of signaling between the visited network and the visited network of the subscriber.

Jonathan: My view is that these types of notifications aren't related to SIP – they are pure bearer notification – right answer is bearer notification protocol of giving failure of resources. That is really my opinion.

Dave Oron: Difficult to believe that you can't do proper scheduling and metering of the bottleneck access links without having some kind of reservation protocol that works over the access links.

Jonathan: They do.

Dave: And obviously they do. So that thing has a state so if you have some kind of end-to-end reservation protocol that runs on top of that – all you need to do is send that to the other end. You say that the two access networks don't communicate about the state of the bearer today – Why don't you just fix that….. Just has to be "edge" to "edge".

Comment: That doesn't exist today.

Dave: Yes it does. Packet cable has had it for 3 years. Adopt packet cable standards as well.

Hayes: 3GPP bearer allocation is not likely to change.

Dean: What we need to do is split it a part into a number of perhaps different usage cases where we show a particular scenario and the sorts of things (i.e., both end points disconnected from network and someone has to take action). If we work through this with different patterns we will find that there will need to be a couple of different mechanisms that imply the different scenarios. Putting it into one bucket – network initiation and termination – and graceful and ungraceful modes – is sort of co-mingling.

Comment: Agrees. Seems that they have two problems. Stop charging and rest of them is cleanup of state. We may need a couple of mechanisms. Time frame for releasing state is immediately.

Jonathan: If there is a direct bearer path between me and you – I am able to send media to you and you are able to send media to me. How is the call not over from user perspective? Don't understand PDP context model.

Discussion pursued on PDP context model…

Jonathan: Statement was made for meeting requirement of P-CSCF for terminating the call. Agrees with requirement as long as you properly define what you mean by "call". What it really means is that service has to be provided to user – which is a conversational bearer – a time metered service that you want to terminate is that the thing that you want to stop. Of course the operator should be able to stop that from a lot of different points. But ultimately the bearer – you have to be getting at it by going through the signaling. By sending BYE you are communicating to CSCFs to terminate the bearer by sending a BYE over SIP and have it go down. There are other ways to communicate that. The essence of it is NOT in SIP – the essence of it is in the bearer.

Dean: Another "use case" when you are talking to a server platform in middle of core network that doesn't have a radio access channel specifically associated with it. And the user has a free access bearer loses their connection is paying for that conference bridge and there are other users - need to tell conference bridge to hang up on all of them.

Jonathan: Connectivity notification service which is just telling things at bearer connectivity that you just died. There are several implications of lost connectivity. Only implication is not termination of the call. It maybe that some applications require that the users call persist for a longer amount of time because they may come back or something like that. It is almost for the application to say what the implications for the lost of bearer – separate from forceful termination because you don't want the application to use these bearer resources anymore. So that is why to some degree – one is an information notification service – and the other has to have some ability for bearer to tell GGSN to turn that off. These are separate things…

Hayes: What we have is a case of primary requirement is associated with the bearer. When the bearer goes away you want to stop charging. Our cases is when use one PDP context setup with a SIP session – which can do several things which are not visible at the bearer level – known only at SIP level. To know when those things start and stop. The only way you can look at those things is at the SIP level. Again, that is very open to fraud as you basically trusted the UEs (no enforcement). So most of cases it is adequate to have bearer detection method – but others you need to inform CSCFs that their has been a change in connectivity so that they can charge accurately. We have to cover both those cases. Shouldn't say you can't enforce so can't charge. Assumption in 3GPP world has been that if you lose connectivity you don't want to be charged or metered.

Peter: Why is this a big deal for SIP to tear session down? Who sets up session relates to security, etc. There are ways that an intermediary can setup a session. Problem is when user agents at edges setup session – then something else tears it down. This is what makes this problem very difficult. Don't know any way this is legally trackable in SIP. Only way this is going to happen is to strongly couple these intermediaries in middle of network to establishment of session. Or use some other protocol that is associated with the bearer to chop the media out forces UE at the edge to figure out that they need to terminate.

6.3.7 Conclusions on BYE

Allison: Capture architectural difference in perception as the requirements document don't perceive that. If we see it so differently between us, it continues to be a problem of how SIP is used from a security perspective and/or accounting.

Hayes: Capture something about this. Without alternative solution 3GPP will continue to be promiscuous with respect to the BYE.

John: Good idea for service providers who are charging for bearer services to charge for bearer services and not involve other signaling. If they are charging other services as well, than charging should be done at that level.

Jonathan: Accounting is happen at both – bearer and SIP.

John: Some may be based on bearer and some just on services.

Peter: Not propagate outside of 3G network (issue with forged BYE).

Hayes: Only reliable time base charging is at bearer level.

Members attending workshop came up with following conclusions on BYE:

- IETF view is that the only reliable source of time-based information is the bearer layer (accounting can be based on a mixture of signaling and bearer but the accounting for timing needs to be based on the bearer).
- Given that the bearer information needs to be synchronized at both ends of the call, 3GPP considers that there is currently no good alternative to the BYE usage (thus it remained unchanged in Release 5).
- Possible ways forward in Release 6 context:
    - 3GPP will investigate enhancing the requirements so that loss of the bearer results in notifying the UE and other entities in the network
    - IETF will investigate mechanisms that are not unduly high overhead and that allow notifications of changes in bearer

6.4 Deployment issues

Topic: Discussion of .GPRS TLD led by Thomas Narten

Reference Contribution 25

3GPP specs (29.060) call out .gprs top-level domain for GRX. Discussion indicates that this is intended for reference only in the operator systems supporting GPRS roaming using GRX. The only elements on this network are essentially GGSN and SGSN nodes, and all the traffic is tunneled in 3GPP protocols. The GRX system is further specified in GSMA documents IR33 and IR34.

The concern is that this TLD was not appropriately allocated to 3GPP by IANA, and MIGHT be allocated to somebody else someday. This could create conflicts. Furthermore, there is the potential that requests could "leak", loading down the root name servers with bogus requests. This would be greatly aggravated if consumer nodes ever start doing lookups. A clear alternative would be to root the GRX space in a second-level domain such as "grx.org" or "gprs.org". The IETF concern is that this is a clear potential problem.

One speaker pointed out that this was historically driven by the GSM Association, not 3GPP. As it is now a historical issue, it is probably up to the operators to fix it. Discussion centered on how to present this to the operators. A strawman argument raised is that "It works, it's not broke, why fix it". Counterarguments include: Historically, this sort of thing has OFTEN (perhaps even usually) resulted in problems. Suggestion made that IETF should offer up a formal recommendation to the operators, as represented by GSMA.

One operator raised the point that the issue isn't clear to him as an

operator, even after having heard this discussion. After all, this is a private network, and problems would be discovered and fixed quickly of it occurred. Another speaker suggested that we look at pages 28-31 of the referenced report, which may describe the operational problem. According to this report, 12.5% of all queries hitting the root name servers are for bogus TLDs, making a real operational problem (app 6 times the traffic of REAL lookups).

Question from operator: Have there been real problems actually resulting from .gprs? Answer: Not that IETF is aware of. It is just that this is an obvious potential problem that can be easily corrected BEFORE it becomes a real problem. Furthermore, it is important that we correct the perception that .gprs is a real TLD before more specifications start using it, and we should also try to educate the various SDOs on appropriate usage of the global DNS.

Question from operator: Assuming that we registered gprs.org -- wouldn't that mean that things on the internet could look up the GRX servers? Answer: maybe. They would actually receive back a response indicating where to go to ask detailed questions about gprs.org, and it is up to gprs.org to decide how to answer that.

Resolutions reached in official report include 1) 3GPP should not use private TLDs in future specs, 2) IETF should produce a technical recommendation to community, and 3) IETF should work with GSMA to establish a consensus to fix the problem.

Question: Does GRX use public address or private? Answer: we're not sure, but the general belief is that the addresses are public. Comment: The GRX is really a VPN network, using an overlay over public addresses.

Topic: Discussion of IPV6, led by Jonne Soininen

Reference Contribution 18

Slides presented review history of 3GPP's usage of IPV6 in both UE and core network. Discussion of use of IPV4 on Gn tunneling interface indicated some uncertainty as to whether the current specifications call for 4, 6, both, or neither. But IMS specifications clearly call for IPV6. Cooperation history includes RFC 3314 and RFC 3316, with more work in progress covering transition in v6ops WG. This work is nearing completion, and interested parties are encouraged to become involved.

Floor opened for comment:

Comment from chair: It would be good to have specific documents originating in SIP/SIPPING and RTP (AVT) groups that address the IPV6 transition aspects of those protocols. Noted that v6ops design team for 3GPP-specific work has been dissolved, but there would still be interest in pursuing this work. Comment from v6ops chair that it would be useful to have guidance from SIP people, especially for 3GPP specific stuff.

Comment: The reference to V4 traffic in IMS is confusing. Please clarify. Response: The terminals might be dual stack, but any V4 traffic they generate would be not IMS. Noted that there may be requirements from specific operators for V4-based IMSes, but this is completely outside the specifications.

Comment: SIP is not likely to be a major problem area for v6 transition. We've already fixed some of this in SDP. However, as SIP does manipulate addressing elements, it may offer some ways of doing interworking by being aware of version differences and splicing in translators, applying STUN, etc. There probably is a need to do something above the level of v6ops charter in terms of application or environment-specific interactions, and it has been the view of v6ops that this is outside of their scope. However, this MAY also exceed the scope of any single group such as SIP, so we need to be sensitive scoping. General consensus seems to be that SIPPING will attempt to progress something rapidly towards v6ops group. The big issue here is finding available and adequate technical resources. This will be needed in release 6 timeframe by 3GPP, possibly December 2003 or shortly thereafter.

Comment: What is scope? IMS nodes talking to v4 internet nodes? Scope seem to be addressed in the IETF's 3GPP v6ops use-cases document (draft-ietf-v6ops-3gpp-cases).

Comment: 3GPP2 may have different issues, and should be encouraged to get into this too. PP2 is currently specifying dual-stackness.

Resolution: IETF will develop a SIP/SDP/RTP etc. transition story as discussed above. Other conclusions noted in chair's conclusions.

6.5 WLAN Interworking in 3GPP

Discussion of IP-030004 (3GPP System - WLAN Interworking) presented by Martin Harris, Orange on behalf of Telnor

Overview of TR 22.934

- High Level Principles roaming vs. interworking
- 6 Interworking scenarios
- Scenario 2 common access control and charging
- Scenario 3 Access to 3GPP system PS services

Scenario 4 Service Continuity non-transparent
Scenario 5 Service continuity – transparent Question: What service discontinuity is acceptable, Answer: <150 msec
Architectural choices: Tight vs. loose coupling
Loose coupling has better flexibility and scalability. 3GPP chose loose coupling

Question: What is the functionality for hand off in Rel 6, Answer: none, handover not supported in Rel. 6
Question: Where is Authentication in AAA or HLR, Answer. in AAA server, HLR provides Au vectors
Status SA1 & SA2
Release 6 Scenarios 2&3
Release 7 Scenarios 3 and up

SA3 Security Needs: EAP (SIM AKA), AAA, possibly Mobile IP

Comment: 3GPP CN expects a Work Item Description (WID) forthcoming (CN4 March)

Question: Scenario 2 vs. 3 when roaming Answer: IMS Access not included in scenario 2 however proprietary methods may be developed.

Comment: Scenarios have been helpful but features need to be better defined.

Question: Since multiple WLAN types are desired, do we require media independence? Answer: Yes, but different WLAN technologies must provide adequate security

Comment: Significant discussion regarding what was required to support multiple WLAN technologies.

Discussion of IP-030022 (IETF-Status-3GWLAN) presented by Bernard Aboba (Jari Arkko co-author)

Contents of presentation not repeated here

Question: Liveness ? Answer: Exchange has not been replayed

Comment: WLAN security currently very media dependent.

It is unclear if the 3GPP requirement for Diameter to transport keys is allowed in 802.11i?

3GPP will provide similar mechanism as GSM for encryption. Question: Does this require anything from IETF Answer: No it is already built in to EAP.

3GPP has no MAC privacy requirement
No additional authentication req beyond SIM/AKA

Question:. What does sequences are discouraged (Open Technical Issues slide) mean
Answer: Assumes that multiple methods of authentication within EAP

Question:. How does identity protection work in home network? Answer: Network identity is hidden, domain name is in the clear

Question:. Which Division of Responsibilities are problems Answer: Key management & AAA (key wrap)

Comment: 3GPP should have outside validation of their security claims

Question: What extensions might be added to EAP to support WLAN Interworking and why has EAP Group charter not been expanded. Answer: EAP was not envisioned to do multiple things and has some limitations.

Question: What is meant by security claims? Answer: There needs to be some analysis of the properties

Conclusions
- 3GPP Should consider and define their requirements for the WLAN link layers
- 3GPP should initiate a 3 way dialog between 3GPP, IETF, and IEEE 802i
- IETF will address the keywrap question.
- IETF will address EAP-SIM and EAP-AKA
- 3GPP should consider commissioning a review to validate that 3GPP WLAN security meets any security claims made in the referenced EAP specs or IEEE specs (keying framework, EAP-SIM, EAP-AKA methods) and any 3GPP security requirements of set forth for WLAN-3GPP interworking.

6.6 3GPP specific considerations

3GPP Environment and Regulatory Considerations session

Presentation by DeWayne Sennett of AT&T on 3GPP environment issues.
(doc is 3GPP-IETF 6.6, 030002)

- Keep in mind that mobiles have limited processing power, memory,
power. User getting used to 200 hrs. standby, 4 hours talk time
- radio spectrum is expensive/scarce
- operators have/want consistent services among GPRS, EDGE, UMTS
- radio bandwidth not constant - distance/multipath limited
- High latency on 3GPP is 100-500ms. Highly desirable to limit number
of round trips for session setup. Transport delay is significant on
slow links 2.5KB takes over a second to transmit
- Want to use Internet protocols in order to get innovative services,
but can't give up any of the above constraints.

Regulatory Requirements:
- number portability
- emergency calls (with or without SIM/USIM on terminal)
- Priority access - support ETS capabilities for emergency responders
- TTY - support for real-time text conversation and interworking with existing text telephony in PSTN
- Privacy - anonymous calls
- Lawful intercept

Comments:

Peterson: IETF knows a lot of these are requirements for SIP (e.g. emergency calls), Some we understand well like number portability. Working on emergency stuff and TTY. Still working on fundamental components (e.g. location information). Acknowledge that they need to be done.

Sennett: note that the presentation was oriented toward US Requirements

Rohan Mahy: some people think having contradictory requirements is a problem. They are actually valuable, as it helps get good solutions for the general case.

Eric Burger: Lawful intercept may be out of scope for IETF, but is going on elsewhere.

Allison Mankin: IETF didn't say exactly that. Said IETF would publish informational drafts, but would not consider complex mechanisms that make protocols less robust and/or secure.

Hannu: TTY and some others may not be global legal requirements. Do all these things carry over from circuit switched to packet switched domain?

Sennett: still in debate on FCC and other regulatory bodies, but assuming that in the future these will be mandated, so want to make sure they can be supported.

Martin ???: from UK perspective if it looks like a phone and sounds like a phone then it is subject to phone regulation

Presentation on Asian Regulatory Requirements by James Kempf of DoCoMo USA labs. (doc 030026).

- no differences for 3GPP. Abides on IMT-2000 abides by same standards

- nobody asked for TDD, not popular in Japan (allegedly not popular in Europe)

- Significant difference in 802.11a WLAN. Different spectrum allocation, in Japan two bands reserved for 802.11a. One you can do either infrastructure or ad hoc, other you can only do infrastructure. Problem that US regulators put a public safety band right in the middle. Will be difficult to get universal spectrum usage worldwide. Either you have long startup time by listening, or scan in which you can interfere in the part of the spectrum not allowed.

- Additional regulations regarding location privacy - Japanese regulators have discovered and think it may surface more elsewhere. In Japan to get location info you must be authorized. User programs password into terminal and gives it out to authorized servers. More complex technique as well - attempt to access location data gives notice to user. User can however delegate management of location privacy to network.

Location privacy and IPV6
- topology != geography but...
- f(topology)~=geography possible
- how complex is it for unauthorized user to deduce f()
- IPv6 deployments that map fixed subnet prefixes to specific geographic areas are at risk.

Duane Sennett: location privacy is one North America concern. Concern not just where you are but where you are not (e.g. not at home).

Kempf: flip side is knowing for legal reasons, murder case guy tried to use cell phone to claim he was not at home. Phone logs proved otherwise

Mark Watson: privacy requirements just specific case of general data privacy regulations in Europe.

Hayes: work has just started in 3GPP on this. In addition have national and regional regulations. Good to have cross coordination.

Wohlert: location services requirements for 3GPP in document 22.071

Hayes: long history of work on location in 3GPP

Presentation on IETF initiatives related to wireless messaging by Eric Burger (doc 0300017)

- History in IETF was VPIM, IFAX, IMAPEXT. Handled file formats, content negotiations, voice messaging semantics (reliable delivery, receipts, message contexts).
- Formed WG called Lemonade to handle diverse service environments.
- link device, etc. have less capability - wireless links, low power handsets
- Enhancements to IMAP4 for steaming multimedia
- enhancements to IMAP4 for low power devices
- server-server bulk message notification
- interoperation with proprietary protocols such as WAP
- Expect liaisons with - 3GPP TSG WG2 SWG3
- In final phases of chartering process

Stephen Hayes: trying to figure out relationship of this with multimedia messaging in 3GPP

Burger: this in support of a number of interfaces in MM1, such as server-server notification. will help on transition 3GPP/3GPP2

General comments:
Mark Watson: tendency to try to eliminate headers to save bandwidth, then sigcomp came along. Need to be careful to make sure compression still works - continued vigilance needed.

Hayes: some limitations will change over time, but some will not.

6.7 Presence & IM

Presentation by Alex Harmand of O2 on Presence and Instant messaging... (doc 03-0008) Snapshot on requirements.

- presence info includes subscriber status, network status, communication means with priority attribute, location information, and free text.
- need efficient way to send presence info on radio interface
- watcher needs way to manage presence list and access to subscriber profile and presence info
- must be able to charge for presence info
- usual authentication and authorization needs.

Showed general architecture slide
IMS messaging requirements
- immediate: no need for negotiation to start message exchange
- session based: agreement and negotiation before exchange
- user experience shall be near real time
- support MIME encoded types - text, picture, etc.
- management and charging

Bearer management is operator concern
- permanent radio bearer must be maintained for the signaling
- no limitation on size of content to be transported by SIPO
- bearer management really complex for good customer experience.
wants approach that can juggle open bearer channels.
Conclusions:
- lot of progress thanks to IETF collaborations
- 3GPP needs further work on profile management and other stuff

Mauricio Arango: what relationship does this have to OSA? Messaging functions there

Harmand: not aware of OSA connection

Drage: In IMS presence work Rel 5 3GPP which has some OSA API elements. In rel.6 there's a task to look at interworking.

Arango: talking about functionality of APIs so providers can deliver these services.

Hayes: OSA a subset of Parlay, so 3GPP one of the active groups in Parlay - these are technology independent APIs. Need mapping to underlying technology. So far not done because service not part of 3GPP rel.5.

Arango: are these independent activities not talking to each other?

Marco ?: these are quite independent activities, maybe there's some interworking activities, but outside the scope of this workshop.

Hayes: didn't preclude, but no current work

?? Nortel: interesting in devices for presence other than mobile telephones. What about other devices - can they be hooked up to 3GPP presence system?

Harmand: haven't considered this yet.

?? Nortel: really vital to include other equipment

Rosenberg: IETF approach is wide - can accommodate this, even can have 3rd party things publishing presence on behalf of other things:

?? Nortel: can have inanimate things with presence too

Rosenberg: absolutely. automata as well

Rosenberg: interesting requirement to have a narrow bearer which you can beef up as needed. This is a natural fit for switching from immediate to session mode.

Presentation by Markus Isomaki on 3GPP/IETF cooperation on SIP-based presence, messaging and conferencing services (doc 030008):

- presence in line with IETF and pretty stable
- IMS messaging will be based on SIP message for immediate, session based with SIP messaging sessions, but deferred delivery with MMS
- IMS group management in process.
- 3GPP requirements on messaging and presence already published as RFCs. Newer stuff already presented in SIMPLE WG.

Showed slide of IMS messaging architecture in rel.6 of 3GPP.

- management interface planned to be based on HTTP, not SIP, e.g. presence list management, and authorization rule manipulation.
- similar approach for conference setup and floor control.
- need to support AKA authentication for this management stuff.
- users in one domain using a conference server in another domain raises some interesting issues.
- still some controversy on partial notification, new drafts appearing now, discussion continues: very useful for wireless environment.
- in 3GPP there is a work item on group management. Same thing going on in IETF SIMPLE WG in items on data manipulation. Coordination useful on this. Requirements now submitted.
- important because mobile devices may need a different interface than a web browser. If you do this, you need a protocol which has to be standardized.
- one proposal: 3GPP will review IETF drafts and make sure it meshes with 3GPP requirements. Can be taken as part of Rel.6, with protocol work some in SIP & SIMPLE in IETF.

Some questions:

- what is process if 3GPP makes extensions to PIDF?
- what about progressing work on partial notifications?
- process for defining extensions to SIP caller prefs and callee capabilities?
- can 3GPP make their own SIP event packages
-

Peterson: PIDF defines its own extensions within it. People encouraged to publish their XML-based extensions. Partial notifications are interesting - won't be done in IMPP but may be done in SIMPLE

Rosenberg: for PIDF - if stuff is generic it ought to be done in IETF and registered. for 3GPP specific (e.g. gprs connected state) can be

done entirely in 3GPP.

Peterson: still should publish public schema and is possible get agreement on common semantics.

Rosenberg: can have interoperability problems with "moods" and stuff like that if you don't register. Better to talk about concrete things rather than talk about this abstractly. Now if good time to get input. On partial notifications concern is getting something that really works - e.g. content indirection may be better for optimizing air interface. For caller prefs - what extensions do you want?

Isomaki: don't know yet.

Rosenberg: can be done with registry via standards track RFC.

Peterson: SIP change defines how to handle things like event packages. Would be curious as to what you have in mind.

Mahy: RFC3427 is SIP change process. Required for event packages that are not standards track has to be something which does not conflict with chartered or planned work. Orthogonal stuff OK.

Mahy: also useful to sort things into baskets with priorities

Garcia: could reach conclusion that 3GPP is actively pursuing these extensions, but isn't aware of active work other than one extension to one package.

Isomaki: agree that not much now, but could be. Would be good to know with plenty of time.

Garcia: reiterate that 3GPP not doing much in the way of extensions at the moment.

Hayes: will do this in principled way - work with IETF. With respect to partial presence update - seems like grudging acceptance by IETF.

Drage: PIDF extension requirements already there in stuff sent to IETF.

Rosenberg: not sure. Please check. Want to see it.

Drage: need 24.831.

Rosenberg: data manipulation is important. not clear that HTTP will suffice - notification capabilities needed that can't be met by

HTTP. Might not be considering the synchronization of lists across devices to tell device that the list has changed and needs to be re-fetched.

Isomaki: problem is that in 3GPP work not far along

Rosenberg: how can you pick a protocol without having the requirements done?

Isomaki: really meant web model, not HTTP specifically.

Rosenberg: is SA2 the place this is being done?

Niemi: decided it should be possible to use HTTP to access the service, but didn't exclude other things. Main point what security mechanisms should be used then said let's look at what's there in IETF. For synch agree you need something more.

Rosenberg: thought ability to do this a huge deal. People prefer functional protocols - would have specific actions for list maintenance rather than just doing web transactions.

Presentation on IETF work on presence and IM by Jon Peterson (doc 0300024)
-will be brief since we already covered most of this
- basis SIP IM and presence are complete
- now assembling related tools to allow creation of complete commercial offerings
- highest priority deliverable for SIMPLE is message sessions.
- also presence publication, PIDF extensions, data manipulation
- working on architecture document for how to assemble all the RFCs to do everything specified
- partial publication and notification
- extensions for things like "other person is typing" notifications
What needed from 3GPP
- priorities from 3GPP on what work is most important, and when needed. Had for rel.5 and provided lots of motivation.
- what is IETF missing?

Drage: always viewed presence stuff (23-041) as what 3GPP wants done first. Already on the dependencies chart
Hayes: have "kiss" draft, been around quite a while. Does this need to be refreshed?

Rosenberg: checked and seems nothing off course. Note to Keith Drage that nothing in there on PIDF extensions. Would like to get to point

where there's a list of documents that 3GPP wants, what it is, and when it's expected. Make sure all requirements are covered.

Hayes: want a list of docs, or capabilities?

Rosenberg: start with capabilities, track with owners

Mankin: document requirements docs were more work than worth. Describing capabilities needed was much more useful. Informal open channel more helpful than potentially stale docs.

Drage: SIMPLE said they wanted generic requirements, and keep 3GPP requirements doc to help with tracking. Seems need another revision of 3GPP reqs. before next IETF meeting, e.g. PIDF extensions.

Peterson: need a matrix more than a document. Need to keep 3GPP requirements from getting "ghetto-ized". Avoids stigma or things like "3G profile".

Isomaki: SIP and SIPPING have had better requirements process than SIMPLE.

Hayes: not sure the difference between capabilities and requirements.

Proposed conclusions:
- 3GPP can extend PIDF, urged to consult with IETF on proposed extensions
- partial notifications an if possible partial publication should be developed by IETF
- IETF should provide feedback to 3GPP on functionality/protocol selections for data manipulation
- 3GPP should refresh presence and messaging requirements and provide priorities and timescales for work
- 3GPP and IETF should work to ensure requirements are covered by work ongoing in IETF.

Peterson: SIMPLE WG not renowned for doing formal requirements docs. Trying to get away from notions like "3GPP profile". There are suitable receptacles for the 3GPP requirement in existing SIMPLE work. May be some use for document for tracking.

Isomaki: couple of new drafts recently published on partial notification/publication which have integrated requirements language.

Hayes: conclusions ok?
...yes.

6.8 IMS Transcoding

Presentation on Transcoding by Gonzalo Camarillo (IP-030023)

- IAB considerations with OPES (RFC3238)
- user requirements for deaf handicapped, etc.
- Things IETF knows: AMR and H.263, MR free, 3GPP2 does not use AMR

Harmand: transcoding needed when two ends do not have the same codec

Garcia: also looking a wide range of applications, speech to text, etc.

Drage: 3GPP should be looking at this.

Peterson: what are 3GPP intentions on transcoding of stuff in SIP
- bodies (e.g. JPEGs in MIME bodies)
-

Drage: part of resource function responsible for transcoding. Doesn't
- say anything about when or how
-

Burger: can't do what you want to with current interfaces. Also point
- out that content transformation is going on in OPES
-

Isomaki: transcoding of message bodies has not been discussed, but similar service in MMS so there is likely to be interest.

Burger: this is about real time rather than bulk.

Mankin: OPES in concerned about multiple protocols

Peterson: seems to remember a document from Nokia in SIPPING. Got
- kicked over to OPES.
-

Isomaki: Nokia doc was direct input to IETF, not through 3GPP.

Hayes: Seems this is an area that hasn't gotten as much attention as it should. Need to look at consent issues identified for OPES. If not, there will be a major disconnect

Camarillo: when network makes assumptions about what user wants, they are usually wrong.

Drage: there is knowledge of users intent via subscription.

Camarillo: sure.

Proposed conclusions:
- 3GPP needs to provide transcoding requirements to IETF.

6.9 Other technical issues

Hayes: the AAA credit control draft and multimedia app are needed for Rel 6. What is their status?

Aboba: AAA multimedia draft and credit control draft would be chartered contingent on finishing Nasreq and more progress on Ipv4.

Aboba: Work on the AAA drafts should continue independently of whether they are chartered.

Aboba: Resource commitment is necessary to initiate the work.

Narten: Supports the idea that if companies feel the work is necessary to do, they should be willing to commit the necessary high quality resources to complete the work.

Conclusions:
- 3GPP is requested to provide necessary resources to complete the AAA drafts

7 Wrap-up and Conclusions

See IP-030029 for conclusions.