3GPP SECURITY STANDARDIZATION

Presentation at Aalto University, December 1, 2016

Vesa Lehtovirta
Ericsson Security Research, NomadicLab
VESÁ LEHTOVIRTA

› Master of Science (MSc. E.E.)
  – Aalto University (previous TKK) 1998

› Master Researcher, Ericsson Security Standards Coordinator
  – Ericsson Security Research

› Standardization delegate in 3GPP security WG (SA3)
  – Security WG (SA3) 2003 - 2016
  – Ericsson lead delegate in SA3
AGENDA

› What is 3GPP and how it works
› 3GPP specifications
› 3GPP and IETF relation
› Security group SA3 and security standards in 3GPP
INTRODUCTION

› While IETF is the organization that creates internet standards, 3GPP is the organization that specifies mobile network standards

› 3GPP specifies mobile network **systems**
  - 3G/UMTS, 4G/LTE/EPC, ….. 5G/NextGen
  - IMS
  - …

Figure source: Wikipedia
3rd Generation Partnership Project (3GPP)

- Formed 1998 by regional telecommunications standard development organizations
  - ARIB, ATIS, CCSA, ETSI, TTA, TTC
  - 3GPP Organizational partners
- Individual companies participate in 3GPP based on membership in 3GPP Organizational partners
- 3GPP Organizational partners endorse 3GPP specifications as regional standards
3GPP ORGANIZATION STRUCTURE

PCG - Project Coordination Group
- 3GPP working procedures
- 3GPP economy and HR

TSG – Technical Specification Group
- Work planning and management
  - Start new WIs (Work Items)
  - Status reporting of WIs
  - Starting and closing of releases
- Formal approval of all changes to specifications
- Terms of reference for WGs
- …
## 3GPP ORGANIZATION STRUCTURE

### Project Co-ordination Group (PCG)

<table>
<thead>
<tr>
<th>TSG RAN</th>
<th>TSG SA</th>
<th>TSG CT</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Radio Access Network</strong></td>
<td><strong>Service &amp; Systems Aspects</strong></td>
<td><strong>Core Network &amp; Terminals</strong></td>
</tr>
<tr>
<td><strong>RAN WG1</strong></td>
<td><strong>SA WG1</strong></td>
<td><strong>CT WG1</strong></td>
</tr>
<tr>
<td>Radio Layer 1 spec</td>
<td>Services</td>
<td>MM/CC/SM (Iu)</td>
</tr>
<tr>
<td><strong>RAN WG2</strong></td>
<td><strong>SA WG2</strong></td>
<td><strong>CT WG3</strong></td>
</tr>
<tr>
<td>Radio Layer 2 spec</td>
<td>Architecture</td>
<td>Intereworking with external networks</td>
</tr>
<tr>
<td>Radio Layer 3 RR spec</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RAN WG3</strong></td>
<td><strong>SA WG3</strong></td>
<td><strong>CT WG4</strong></td>
</tr>
<tr>
<td>lub spec, lur spec, lu spec</td>
<td>Security</td>
<td>MAP/GTP/SC/HS</td>
</tr>
<tr>
<td>UTRAN O&amp;M requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RAN WG4</strong></td>
<td><strong>SA WG4</strong></td>
<td><strong>CT WG6</strong></td>
</tr>
<tr>
<td>Radio Performance</td>
<td>Codec</td>
<td>Smart Card Application Aspects</td>
</tr>
<tr>
<td>Protocol aspects</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RAN WG5</strong></td>
<td><strong>SA WG5</strong></td>
<td></td>
</tr>
<tr>
<td>Mobile Terminal</td>
<td>Telecom Management</td>
<td></td>
</tr>
<tr>
<td>Conformance Testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RAN WG6</strong></td>
<td><strong>SA WG6</strong></td>
<td></td>
</tr>
<tr>
<td>Legacy RAN radio and protocol</td>
<td>Mission-critical applications</td>
<td></td>
</tr>
</tbody>
</table>

WG – Working groups

Actual technical work
3GPP WGs MAPPED TO LTE/EPS
ARCHITECTURE, RESPONSIBLE WGS AND DEVELOPMENT STAGES

Stage 1
- SA1: Service requirements
- SA2: Architecture

Stage 2
- SA3: Security
- SA4: Codecs
- SA5: O&M and Charging
- SA6: Critical communications

Stage 3
- UICC
- UE

External PDN

SYSTEM (EPS, UMTS)
CORE NW (EPC, GPRS)
RAN (E-UTRAN, UTRAN, GERAN)
S-Gw
P-Gw
MME
HSS

SA1: Service requirements
SA2: Architecture
SA3: Security
SA4: Codecs
SA5: O&M and Charging
SA6: Critical communications
A 3GPP RELEASE

› A release provides developers with a stable platform for implementation and to allow for the addition of new features required by the market.
› Roughly one Release per year. Rel-99 was the first, followed by Rel-4, … now Rel-14 ongoing.
› A set of new features developed within a corresponding set of 3GPP Work Items.
› Copy of specifications from last release created with release number incremented. Ensures backwards compatibility.
› When the work is reasonably complete and stable the release is Frozen
  – After freeze no new functionality can be introduced but corrections can still be made
3GPP DECISIONS

› 3GPP decisions are made in the meetings
› 3GPP decisions primarily based on consensus
  – Consensus primarily reached based on technical discussions
    › Performance vs complexity (vs security) of solutions
    – Informal methods like ‘show of hands’ can be used to reach consensus
› ‘Working agreements’ can be used as ‘tentative decisions’ when consensus can not be reached
  – Used when there is clear majority for the decision but there is sustained objection from a small minority of companies
› If consensus can not be reached, decisions can be taken by formal voting
  – Rarely used
  – Requires 71% majority
  – A working agreement that is ‘challenged’ is escalated to voting
A year according to 3GPP

1. **3GPP Plenaries**
   - In December
   - In March
   - In June

2. **3GPP working groups**
   - Meets 1-2 times between each 3GPP plenary.
   - Each meeting is typically 5 days long.
   - Change Requests (CR) are AGREED in the working groups and sent to the next plenary for APPROVAL.

---

© Ericsson AB 2016 | 2016-11-29 | Page 11
3GPP SPECIFICATIONS

› Specifications are the output of 3GPP
› 3GPP has two types of specifications
  – Technical Specifications (TSs) are THE normative specifications, i.e. standards
  – Technical Reports (TRs) are studies and guidelines. They are usually informative
› The work on normative TS is usually preceded by study phase which produces a TR.
  – E.g. 4G security standard TS 33.401 was preceded by study in TR 33.821.
› Specifications are “owned” by a WG
› Specifications evolve thru Releases when new features are added.
## 3GPP SPECIFICATIONS

> All 3GPP specifications are publicly available at [http://www.3gpp.org/specifications/specifications](http://www.3gpp.org/specifications/specifications)

<table>
<thead>
<tr>
<th>Subject of specification series</th>
<th>3G and beyond / GSM (R99 and later)</th>
<th>GSM only (Rel-4 and later)</th>
<th>GSM only (before Rel-4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>General information (long defunct)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Requirements</td>
<td>21 series</td>
<td>41 series</td>
<td>01 series</td>
</tr>
<tr>
<td>Service aspects (&quot;stage 1&quot;)</td>
<td>22 series</td>
<td>42 series</td>
<td>02 series</td>
</tr>
<tr>
<td>Technical realization (&quot;stage 2&quot;)</td>
<td>23 series</td>
<td>43 series</td>
<td>03 series</td>
</tr>
<tr>
<td>Signalling protocols (&quot;stage 3&quot;) - user equipment to network</td>
<td>24 series</td>
<td>44 series</td>
<td>04 series</td>
</tr>
<tr>
<td>Radio aspects</td>
<td>25 series</td>
<td>45 series</td>
<td>05 series</td>
</tr>
<tr>
<td>CODECs</td>
<td>28 series</td>
<td>46 series</td>
<td>06 series</td>
</tr>
<tr>
<td>Data</td>
<td>27 series</td>
<td>47 series (none exists)</td>
<td>07 series</td>
</tr>
<tr>
<td>Signalling protocols (&quot;stage 3&quot;) - {RS-CN} and OAM&amp;P and Charging (overflow from 32 - range)</td>
<td>28 series</td>
<td>48 series</td>
<td>08 series</td>
</tr>
<tr>
<td>Signalling protocols (&quot;stage 3&quot;) - intra-fixed-network</td>
<td>29 series</td>
<td>49 series</td>
<td>09 series</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject of specification series</th>
<th>3G and beyond / GSM (R99 and later)</th>
<th>GSM only (Rel-4 and later)</th>
<th>GSM only (before Rel-4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programme management</td>
<td>30 series</td>
<td>50 series</td>
<td>10 series</td>
</tr>
<tr>
<td>Subscriber Identity Module (SIM / USIM), IC Cards. Test specs</td>
<td>31 series</td>
<td>51 series</td>
<td>11 series</td>
</tr>
<tr>
<td>OAM&amp;P and Charging</td>
<td>32 series</td>
<td>52 series</td>
<td>12 series</td>
</tr>
<tr>
<td>Access requirements and test specifications</td>
<td>13 series (1)</td>
<td>13 series (1)</td>
<td></td>
</tr>
<tr>
<td>Security aspects</td>
<td>33 series</td>
<td>(2)</td>
<td>(2)</td>
</tr>
<tr>
<td>UE and (U)SIM test specifications</td>
<td>34 series</td>
<td>(2)</td>
<td>11 series</td>
</tr>
<tr>
<td>Security algorithms (3)</td>
<td>35 series</td>
<td>55 series</td>
<td>(4)</td>
</tr>
<tr>
<td>LTE (Evolved UTRA), LTE-Advanced, LTE-Advanced Pro radio technology</td>
<td>36 series</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Multiple radio access technology aspects</td>
<td>37 series</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Radio technology beyond LTE</td>
<td>38 series</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
3GPP WGS AND SPECIFICATIONS
EXAMPLE FOR LTE

Stage 1
- SA1: Service requirements 22-series
- SA2: Architecture 23-series

Stage 2
- SA3: Security 33-series
- SA4: Codecs 26-series
- SA5: O&M and Charging 28 & 32 series

Stage 3
- CT6 31-series
- CT1 24-series
- CT4 29-series
- CT3
- RAN (E-UTRAN, UTRAN, GERAN)
- CORE NW (EPC, GPRS)

SYSTEM (EPS, UMTS)

External PDN
3GPP SPECIFICATION NUMBERING

› 3GPP TS XX.YYY version Z1.Z2.Z3
› XX gives the specification series or area, and indicates WG ownership
  – E.g. 33 series are the security standards
› YYY indicates the specification number
  – 7xx, 8xx, and 9xx series are for TRs, other series are for TSs.
› Z1.Z2.Z3, indicates the version, where
  – Z1 indicates Release
  – Z2 indicates version within a Release
  – Z3 indicates a minor editorial change
COMMON DOCUMENT TYPES

› **Work item:** All work within a standardisation working group should be based on Work Items that describe the justification, scope and expected output. The document describing this is called a Work Item description (WID).

› **Discussion paper:** A discussion paper usually is used for justification or giving more explanation of a proposal.

› **Pseudo CR (pCR):** A pCR is a suggested change to a draft specification or report.

› **Change Request (CR):** A CR is a suggested change to an approved specification or report.

› **Liaison Statement (LS):** An LS is the same as an official letter or mail from one standardization working group to another. The LS is often used to send questions, share information and to draw another group’s attention to a particular subject or decision.

› **Contribution:** All of the above are commonly called as Contributions.

› **3GPP is contribution driven:** All work is based on contributions from member companies.
The working group develops the draft with pseudo CRs until ~80% ready.

The plenary will approve the TS and includes it in the current release. It is placed under change control and maintained with the help of CRs.
3GPP - IETF RELATION

› 3GPP uses extensively IETF protocols. Most protocols above IP layer used in 3GPP have been defined in IETF.

› In addition to using IETF protocols, 3GPP and IETF are doing collaboration to specify needed protocols for 3GPP, e.g.
  – HTTP Digest AKA (RFC 3310), which is embedding 3GPP AKA to HTTP digest (RFC2617)
  – EAP-AKA (RFC 4187) and EAP-AKA’ (RFC 5448), which define 3GPP AKA -based EAP methods for EAP (RFC 3748)

› Both organizations have a liaison officer to coordinate the co-operation
### 3GPP SA3

#### Project Co-ordination Group (PCG)

<table>
<thead>
<tr>
<th>TSG RAN</th>
<th>TSG SA</th>
<th>TSG CT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radio Access Network</td>
<td>Service &amp; Systems Aspects</td>
<td>Core Network &amp; Terminals</td>
</tr>
<tr>
<td>RAN WG1</td>
<td>SA WG1</td>
<td>CT WG1</td>
</tr>
<tr>
<td>Radio Layer 1 spec</td>
<td>Services</td>
<td>MM/CC/SM (Iu)</td>
</tr>
<tr>
<td>RAN WG2</td>
<td>SA WG2</td>
<td>CT WG3</td>
</tr>
<tr>
<td>Radio Layer 2 spec</td>
<td>Architecture</td>
<td>Interworking with external networks</td>
</tr>
<tr>
<td>Radio Layer 3 RR spec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RAN WG3</td>
<td><strong>SA WG3</strong></td>
<td>CT WG4</td>
</tr>
<tr>
<td>lub spec, Iur spec, lu spec UTRAN O&amp;M requirements</td>
<td><strong>Security</strong></td>
<td>MAP/GTP/BCH/SSi</td>
</tr>
<tr>
<td>RAN WG4</td>
<td>SA WG4</td>
<td>CT WG6</td>
</tr>
<tr>
<td>Radio Performance Protocol aspects</td>
<td>Codec</td>
<td>Smart Card Application Aspects</td>
</tr>
<tr>
<td>RAN WG5</td>
<td>SA WG5</td>
<td></td>
</tr>
<tr>
<td>Mobile Terminal Conformance Testing</td>
<td>Telecom Management</td>
<td></td>
</tr>
<tr>
<td>RAN WG6</td>
<td>SA WG6</td>
<td></td>
</tr>
<tr>
<td>Legacy RAN radio and protocol</td>
<td>Mission-critical applications</td>
<td></td>
</tr>
</tbody>
</table>
3GPP SA3 RESPONSIBILITIES

› The WG has the overall responsibility for **security and privacy** in 3GPP systems
  - performs analysis of potential threats to these systems
  - determines the security and privacy requirements for 3GPP systems
  - specifies the security architectures and protocols
  - ensures the availability of cryptographic algorithms which need to be part of the specifications

› SA3 has tight collaboration with ETSI SAGE (*Security Algorithms Group of Experts)*
  - ETSI SAGE is responsible for specifying and evaluating the cryptographic algorithms for 3GPP

› SA3 has a chairman and two vice-chairmen
› SA3 has roughly 50-60 attendees per meeting
"WORKING AREAS" IN 3GPP SECURITY OVERVIEW

Security for Applications (GBA, Generic Bootstrapping Architecture)
(Mission Critical Push to Talk)

"Network domain security"

IMS security

"Security assurance"

"Privacy"

Access security

"Devide to Device / Proximity Services"
3GPP SA3 SPECIFICATIONS

› Security specifications are series 33.xxx
› Examples of 3GPP security specifications
   – TS 33.102 UMTS security specification
   – TS 33.401 EPS security specification
   – TS 33.210 Network Domain Security
   – TS 33.203 IMS security
   – TS 33.220 Generic Bootstrapping architecture
   – ...

› All SA3 specifications are publicly available at http://www.3gpp.org/DynaReport/33-series.htm
A BUILDING BLOCK: 3GPP AKA

- Authentication and Key Agreement algorithm, a.k.a. AKA
  - Algorithm to authenticate the identity on the USIM/UICC to the network and vice versa
  - Visited network asks for authentication vectors from home network
  - Visited network authenticates the UE
  - Provides keys as a by-product which can be used to protect communication
USES OF AKA IN 3GPP SECURITY

- **HTTP digest AKA** for GBA
- **HTTP digest AKA** for IMS
- **2G AKA**
- **3G AKA**
- **EAP SIM**
- **EAP AKA**
- **EPS AKA**
- **EAP AKA’**

Security for Applications (GBA, Generic Bootstrapping Architecture)
(Mission Critical Push to Talk)

NAF
BSF

IMS security
P-CSCF
S-CSCF

HSS

2G core
3G core
EPS core
WLAN
UTRAN
GERAN
non3GPP access
Access security

© Ericsson AB 2016 | 2016-11-29 | Page 24
LTE SECURITY MECHANISMS SIMPLIFIED GLIMPSE FROM TS 33.401

› Authentication between UE (USIM) and MME
› Ciphering and integrity protection of core network (NAS) signalling between UE and MME
› Ciphering and integrity protection of radio (RRC) signalling between UE and eNB
› Ciphering of user plane data between UE and eNB
› Ciphering of user plane data by IPsec between eNB and S-GW
› Privacy by usage of temporary identifiers
5G WORK

› Work on 5G standardization is ongoing in 3GPP
  – Study phase is concluding and normative specifications of phase 1 planned for Q1-Q2 2018

› Main areas of work
  – Enhanced Mobile Broadband
  – Massive scale IoT
  – Critical communications

› Stage 1:
  – Requirements group SA1 has concluded their studies and normative requirements are being specified

› Stage 2:
  – Architecture group SA2 is concluding study in TR 23.799 and starting normative work
  – Security group SA3 concluding study by March 2017 in TR 33.899
  – RAN (Radio) groups working on studies in 38.xxx series TRs
SOURCES OF INFORMATION

› 3GPP website: www.3GPP.org
› Ericsson Technology review: https://www.ericsson.com/thecompany/our_publications/ericsson_technology_review
› Ericsson 5G security white paper
› http://www.ericsson.com/res/docs/whitepapers/wp-5g-security.pdf