CELTIC
Telecommunication Solutions

MEVICO
Mobile Networks Evolution for Individual Communications Experience

EUREKA

# Performance and suitability analysis of HIP-based lightweight user authentication method


WP2

BME-MIK, CWC

Zoltán Faigl, Jani Pellikka, László Bokor, Andrei Gurtov

zfaigl@mik.bme.hu


Mobile Innovation Centre

CWC CENTRE FOR WIRELESS COMMUNICATIONS
University of Oulu

# Outline

Performance evaluation of HIP Diet Exchange with AKA authentication

- Objectives
- Compared technologies
- Validation scenarios, testbed, expected results
- Performance measurement results, and their relevance to 3GPP EPC
- Conclusions

Suitability analysis under multiple criteria

- Objectives
- Methodology
- Results
- Conclusions

- Future work

# Objectives

- Challenges:
  - With the realization of Internet-of-Things we expect new applications requiring high security and deployment in ressource constrained UEs.
    - E.g. M2M communication related usage scenarios will contain a subset of monitoring and controling applications that will communicate over 3GPP architecture and will require high security.
  - 3GPP and non-3GPP accesses provide different set of security services. An important objective is to provide unified security services, independent of the access
  - Reduction of security setup overhead
  - Seamless interworking with different access technologies for improved real time connection continuation
  - Seamless handovers

# Objectives (cont.)

- Objectives
  - Improve the performance of initial attachment phase (authentication).
  - The results are expected to support our decisions on which technologies and authentication methods should be selected in distributed EPC where the first IP gateway may be located in the national, regional, or local Point of Presence (POP).
  - Examine whether seamless handover is achievable (without doing any further optimization, e.g. context transfer to new GW, etc.)
- Investigated technology
  - Host Identity Protocol (HIP) Diet Exchange with and without AKA (referred to as ***DEX*** and ***DEX-AKA***)
  - Comaprison base: Internet Key Exchange version 2 (IKEv2) with ***EAP-AKA***, ***EAP-TLS***, Pre-shared key (***PSK***) and HIP Base Exchange (***BEX***)

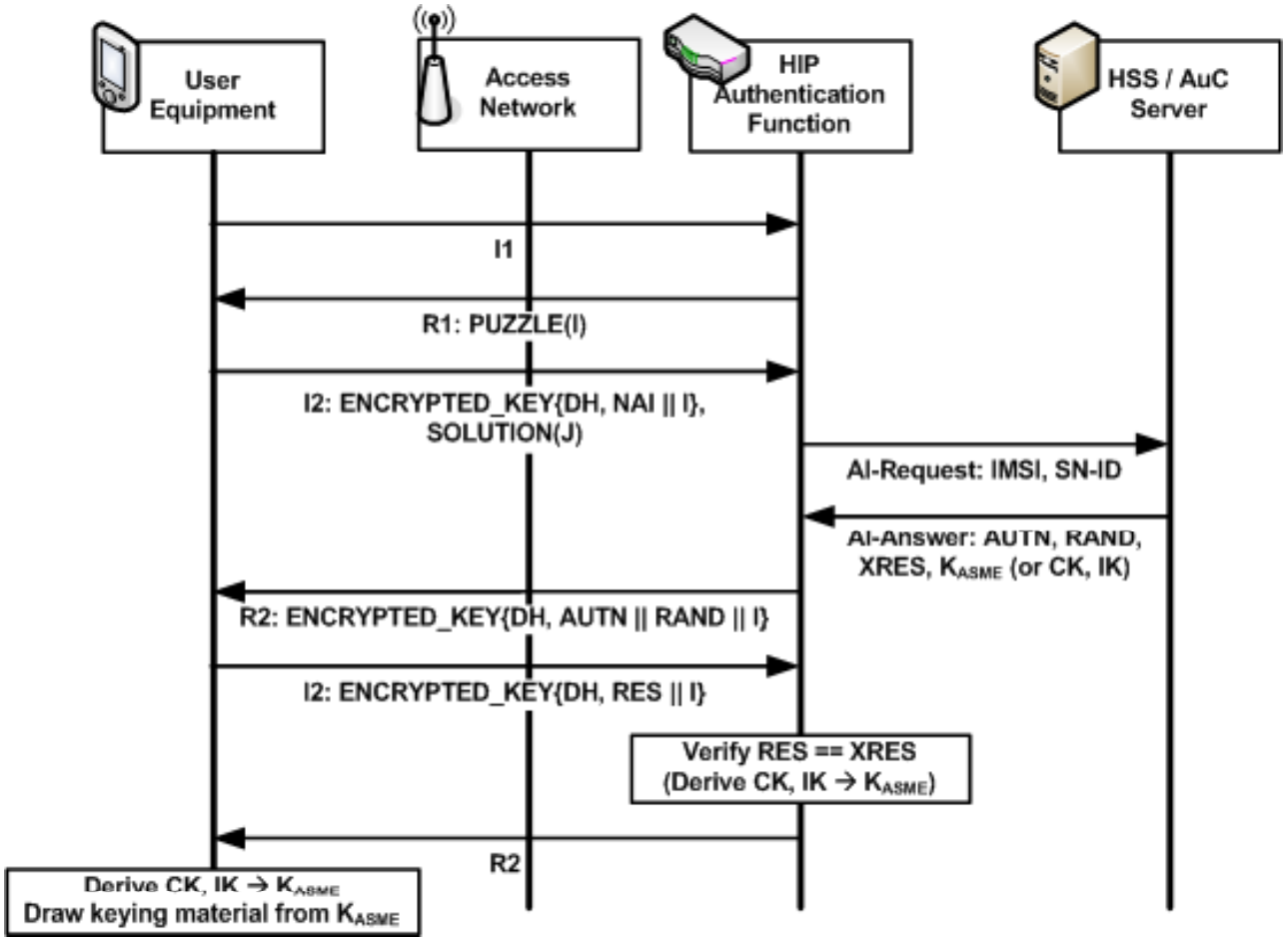
# Technologies, contributions

- HIP DEX-AKA provides similar functionality as the Internet Key Exchange protocol v2 (IKEv2) with EAP-AKA
  - Both technologies provide mutual authentication and establish an IPsec security association pair to protect the path between the UE and the ePDG in the network layer
- Application area:
  - controls user access authentication and authorization of USIM based UEs in non-managed non-3GPP access networks
  - DEX AKA is intended to be applied as a uniform L3 authentication service on the top of disparate access networks in a distributed/flat EPC, because the different L2 authentication methods provide different security services.

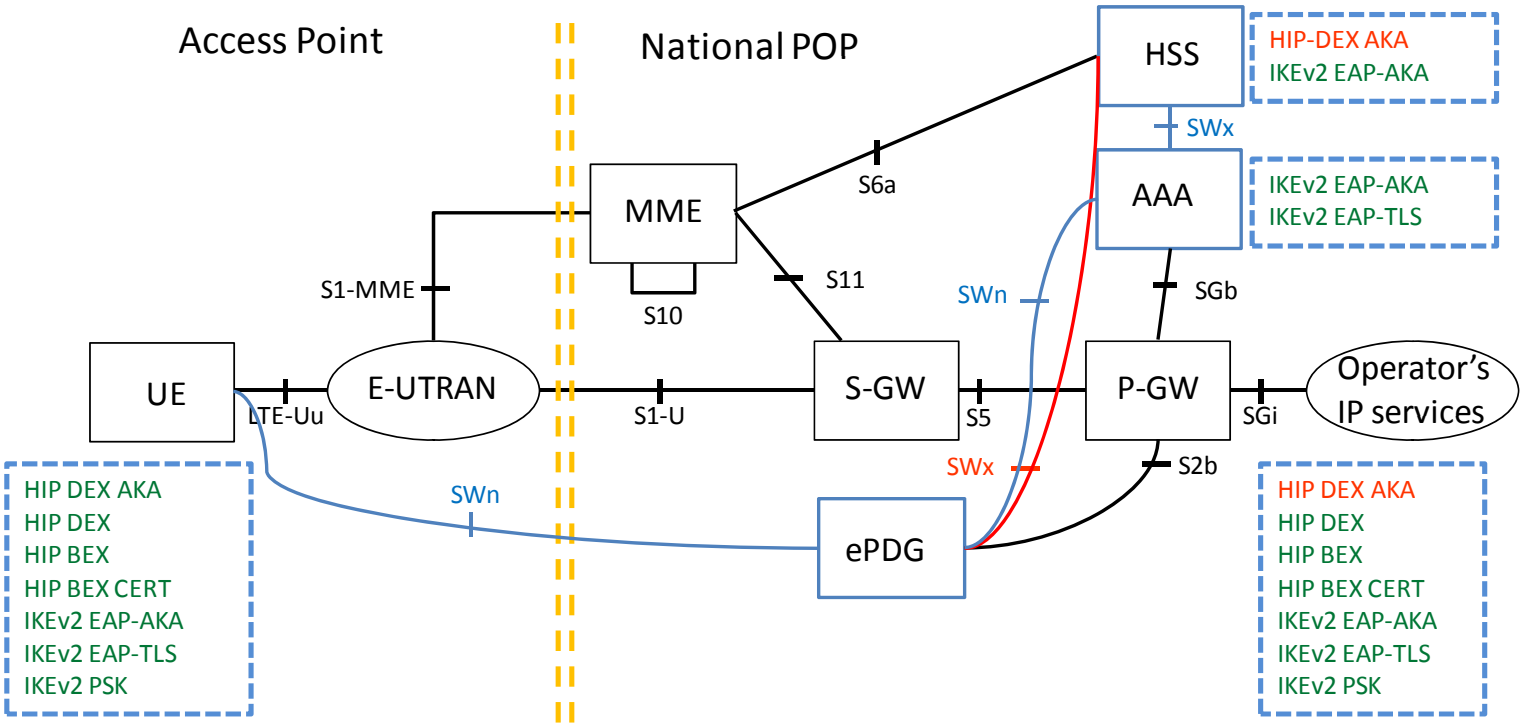
# Compared technologies

- HIP DEX, HIP DEX AKA:
  - C++ prototype (CWC)
- IKEv2 with PSK, EAP-AKA, EAP-TLS:
  - strongSwan with modifications to support EAP-AKA using the test USIM cards of MIK (MIK)
- HIP:
  - InfraHIP
- Authentication service:
  - freeRadius, with modifications to support EAP-AKA with Huawei HSS9820 (MIK).

# HIP Diet Exchange with EPS AKA authentication

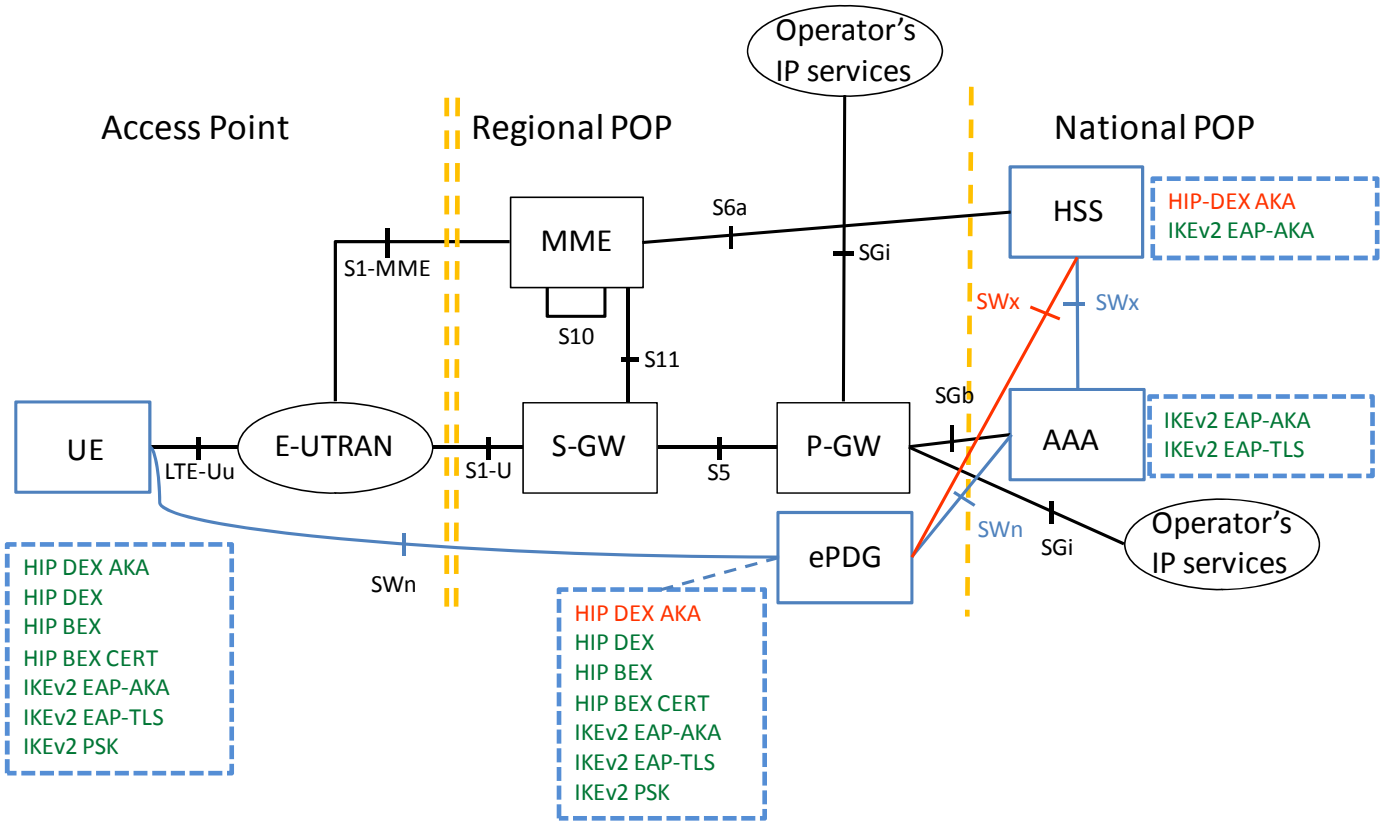


# Reference scenarios



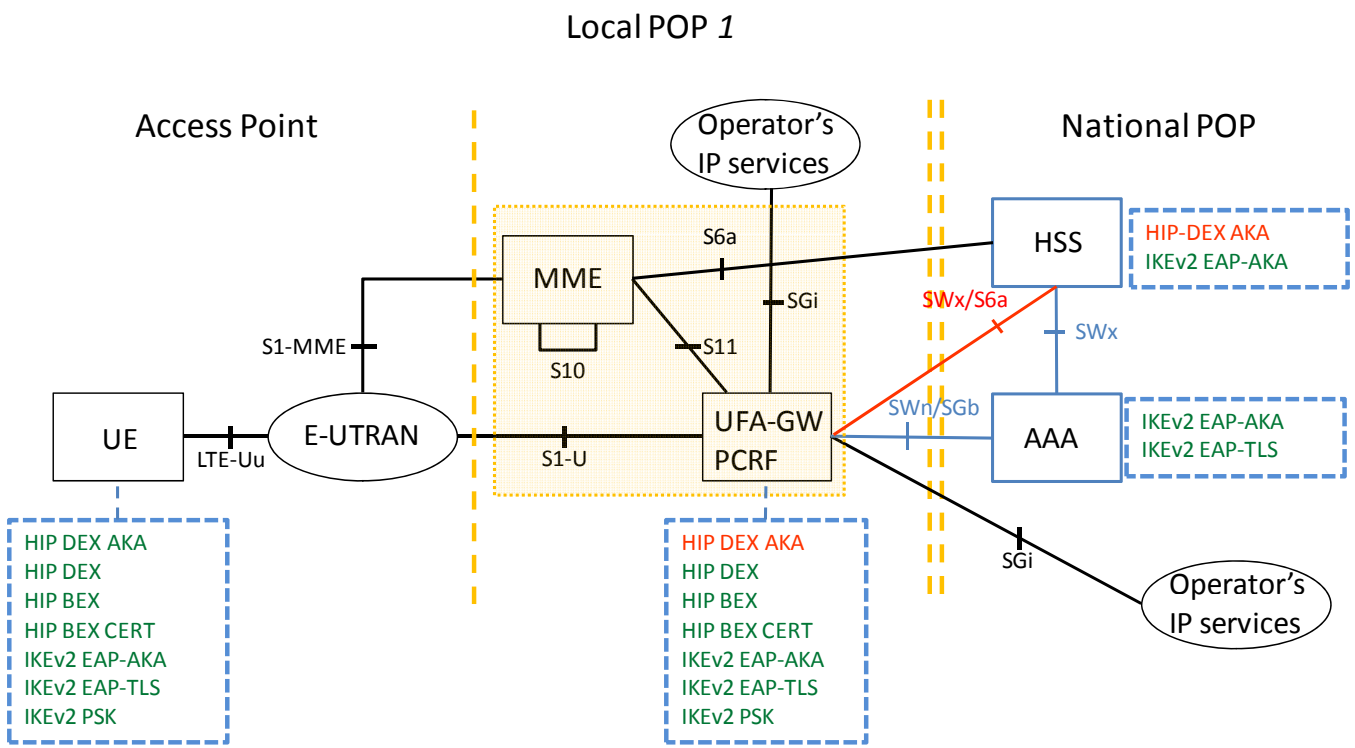

Centralized

# Reference scenarios



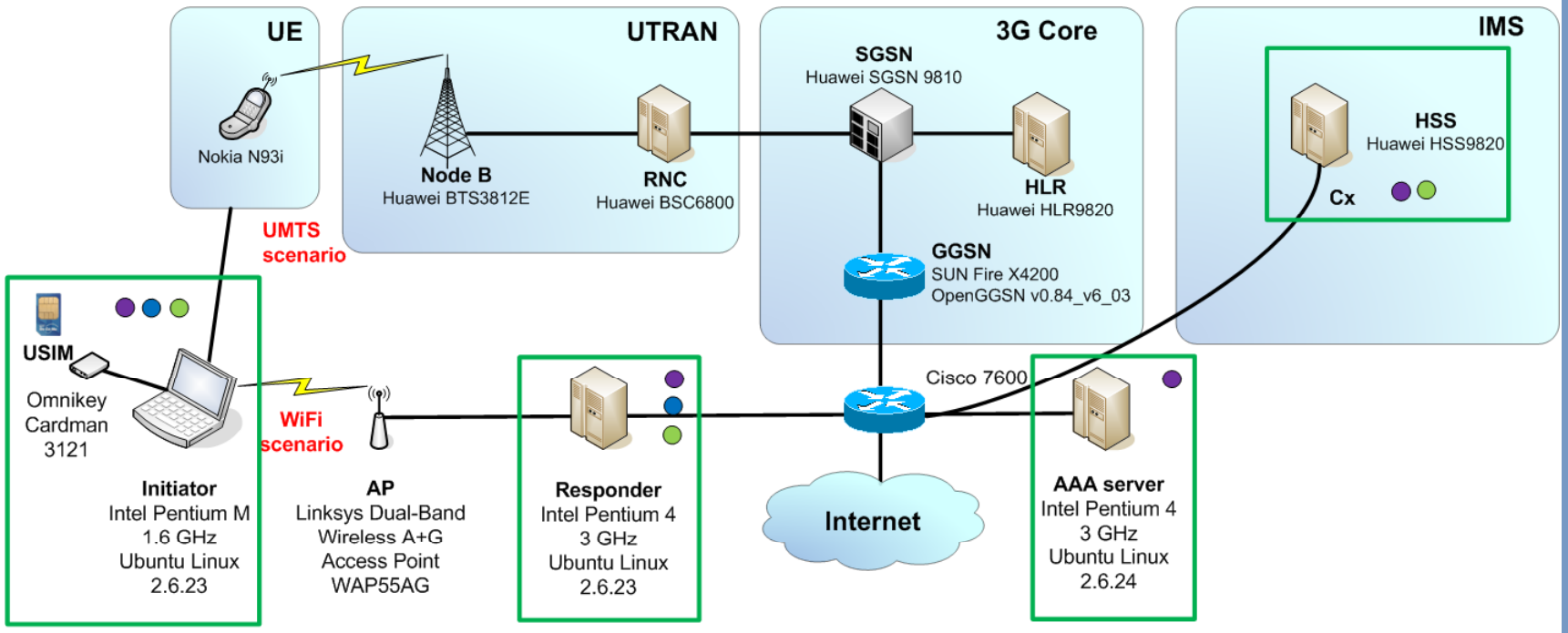

Distributed

# Reference scenarios




Flat

# Validation environment




| | centralized | distributed | flat |
|---|---|---|---|
| **UE - P-GW/ePDG/SGW** | 30 ms | 15 ms | 10 ms |
| **GW - AAA** | 5 ms | 15 ms | 30 ms |
| **AAA - HSS** | 5 ms | 5 ms | 5 ms |
| **GW - HSS** | 5 ms | 15 ms | 30 ms |

# Validation environment

- The L3 authentication delay has been evaluated in all the three reference scenarios using two different access networks
  - WiFi (IEEE 802.21g, 54 Mbps)
  - HSDPA downlink (QPSK, 7.2Mbps) and UMTS uplink (384 kbps). LTE would be more appropriate but is not available in the demonstrator.
- Reference scenarios have been partly emulated by additional (constant) network delays
- Validation tools:
  - netem : emulate longer paths with additional network delays
  - Wireshark : measure authentication flow duration
  - Oprofile in time mode: measure CPU utilization in the UE, GW and AAA server
  - Valgrind massif tool: measure peak stack and heap memory size allocated by the initialization and one authentication flow.
- Comparison based evaluation
  - The influence of specific  environment is hence mitigated.

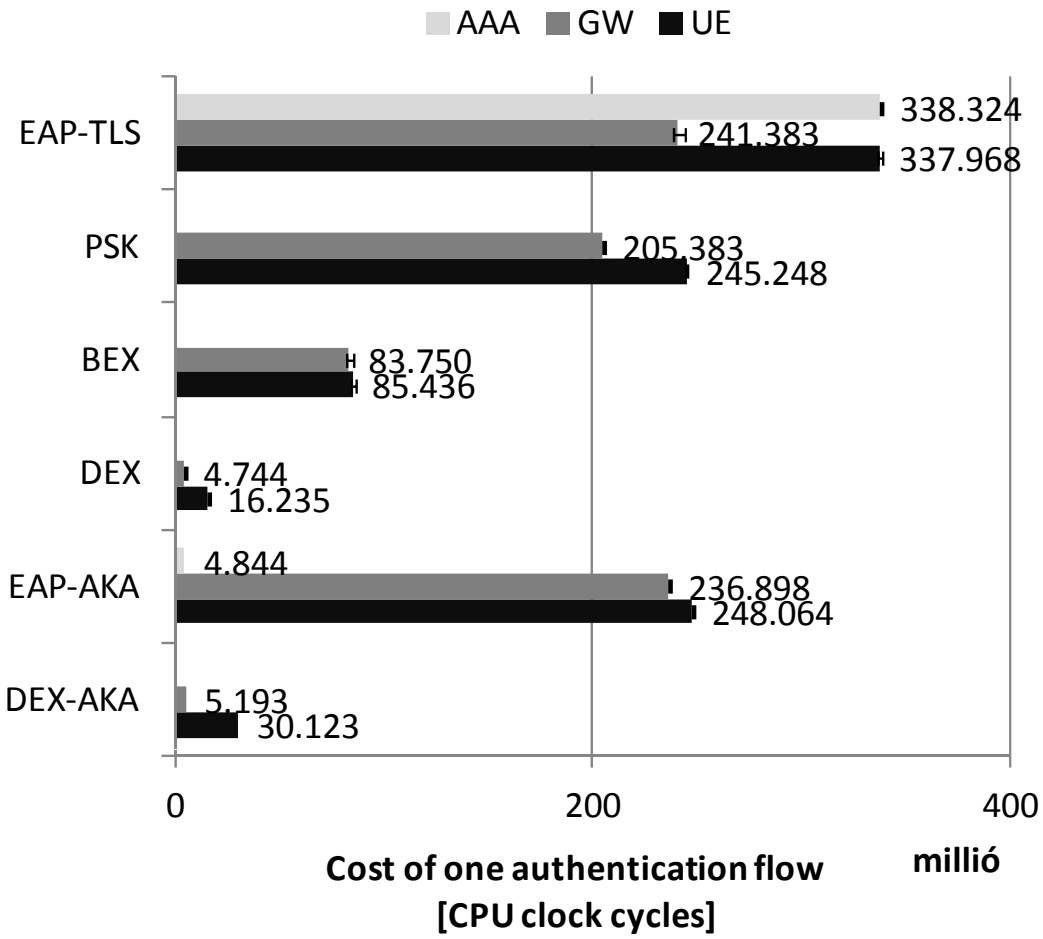
# Expected results, measurement plans

- Reduction of average CPU utilization:
  - measure the CPU clock cycles of one authentication flow
- Reduction of memory utilization:
  - measure the peak heap and stack memory size allocated during the initialization of softwares and one authentication flow
- Reduction of authentication delay (service interruption delay due to full re-authentication):
  - measure the duration of the successful authentication in the network-layer
- Reduction of the number of control messages (utilization of network links):
  - count signalling messages
- The validation aims to show the exact gains in terms of the different KPIs

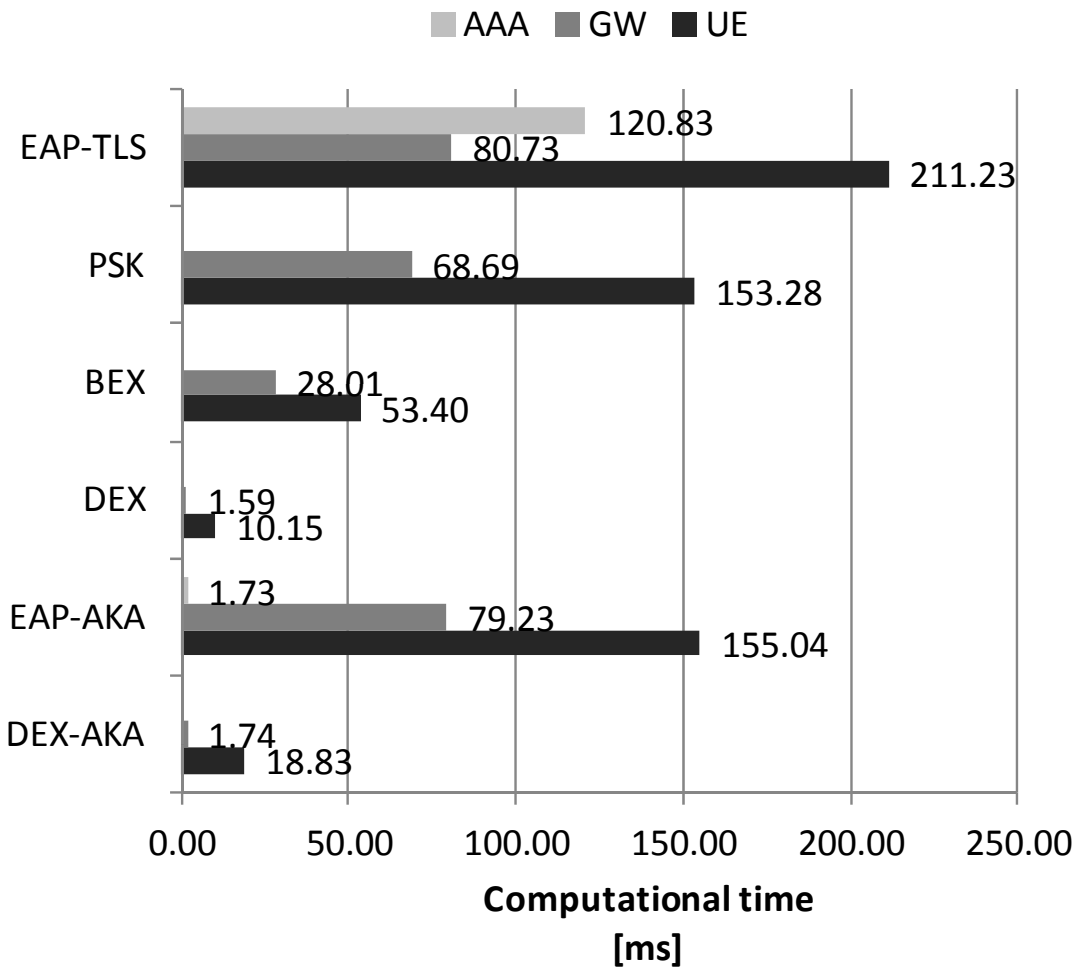
# Results

- CPU cost
- Memory cost
- Authentication delay
- Message complexity
  - Number and size of control messages

# CPU cost


AAA
GW
UE
EAP-TLS
338.324
241.383
337.968
PSK
205.383
245.248
BEX
83.750
85.436
DEX
4.744
16.235
EAP-AKA
4.844
236.898
248.064
DEX-AKA
5.193
30.123
0
200
400
millió
Cost of one authentication flow
[CPU clock cycles]

# Computational times



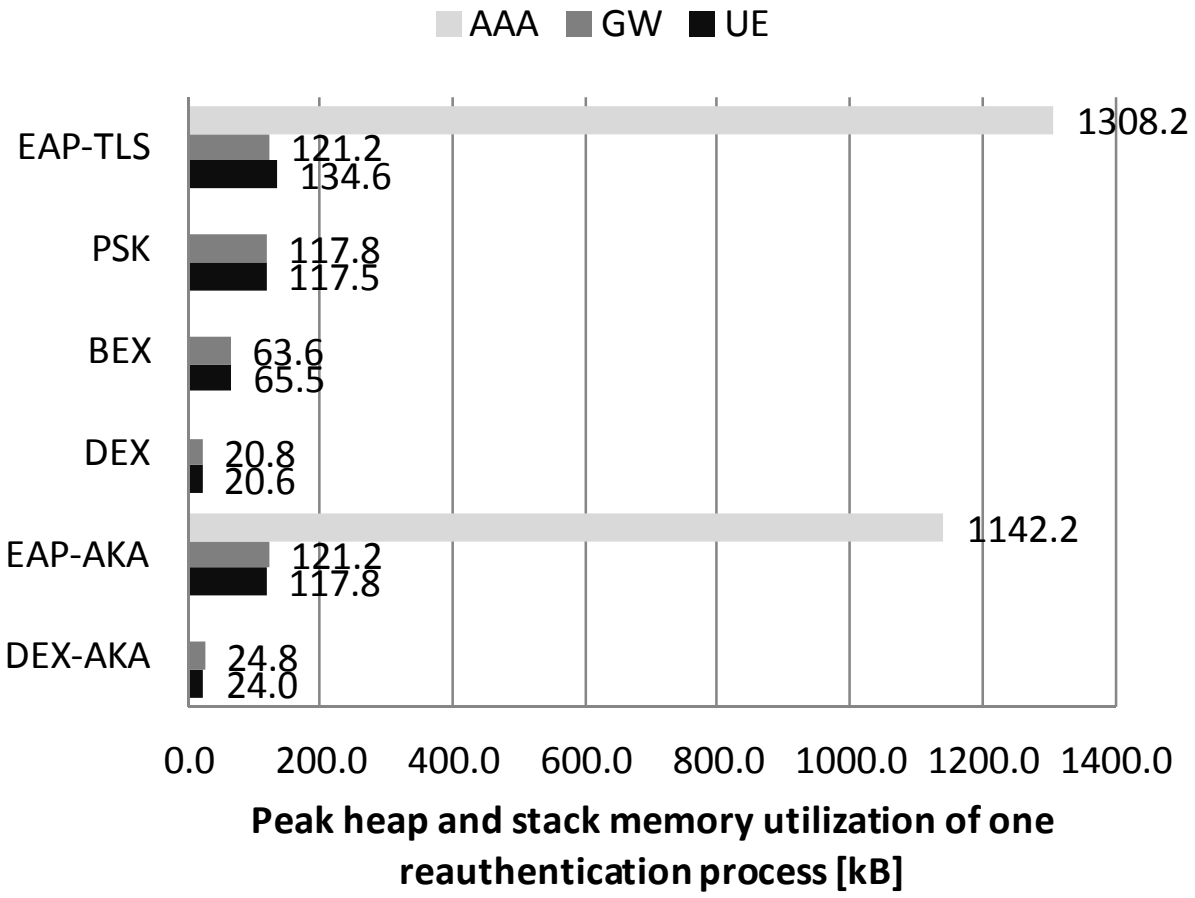
# Proportion of computational delays in the authentication delay

| | centralized | distributed | flat |
|---|---|---|---|
| WiFi access | | | |
| DEX-AKA | 7.1% | 9.3% | 9.4% |
| EAP-AKA | 40.6% | 50.4% | 49.3% |
| DEX | 8.6% | 15.2% | 20.3% |
| BEX | 39.8% | 56.0% | 65.7% |
| PSK | 70.5% | 89.6% | 97.1% |
| EAP-TLS | 39.4% | 45.2% | 39.8% |
| HSDPA/UMTS access | | | |
| DEX-AKA | 3.3% | 3.7% | 3.7% |
| EAP-AKA | 18.5% | 20.3% | 20.0% |
| DEX | 3.2% | 3.9% | 4.1% |
| BEX | 14.3% | 16.1% | 17.0% |
| PSK | 33.3% | 37.5% | 38.8% |
| EAP-TLS | 16.3% | 17.3% | 16.4% |

# CPU cost

- Reduction in the amount of non idle CPU intervals occupied by the authentication process is significant in relative terms (UE: 12%, GW: 2%, DEX-AKA/EAP-AKA)
- In absolute terms, the ferquency and cost of re-authentications is so low, that no significant influence is on the battery consumption of the UE. CPU typically consumes less than 10% of the total energy consumption.
- GW is frequently accessed, must fulfill real-time requirements, hence reduction in CPU capacity allocated for re-authentications is important.
- In case of DEX-AKA the AAA server is not utilized, but HSS is accessed at each authentication run. Scalability issues could be mitigated by including AAA servers also in case of DEX-AKA.

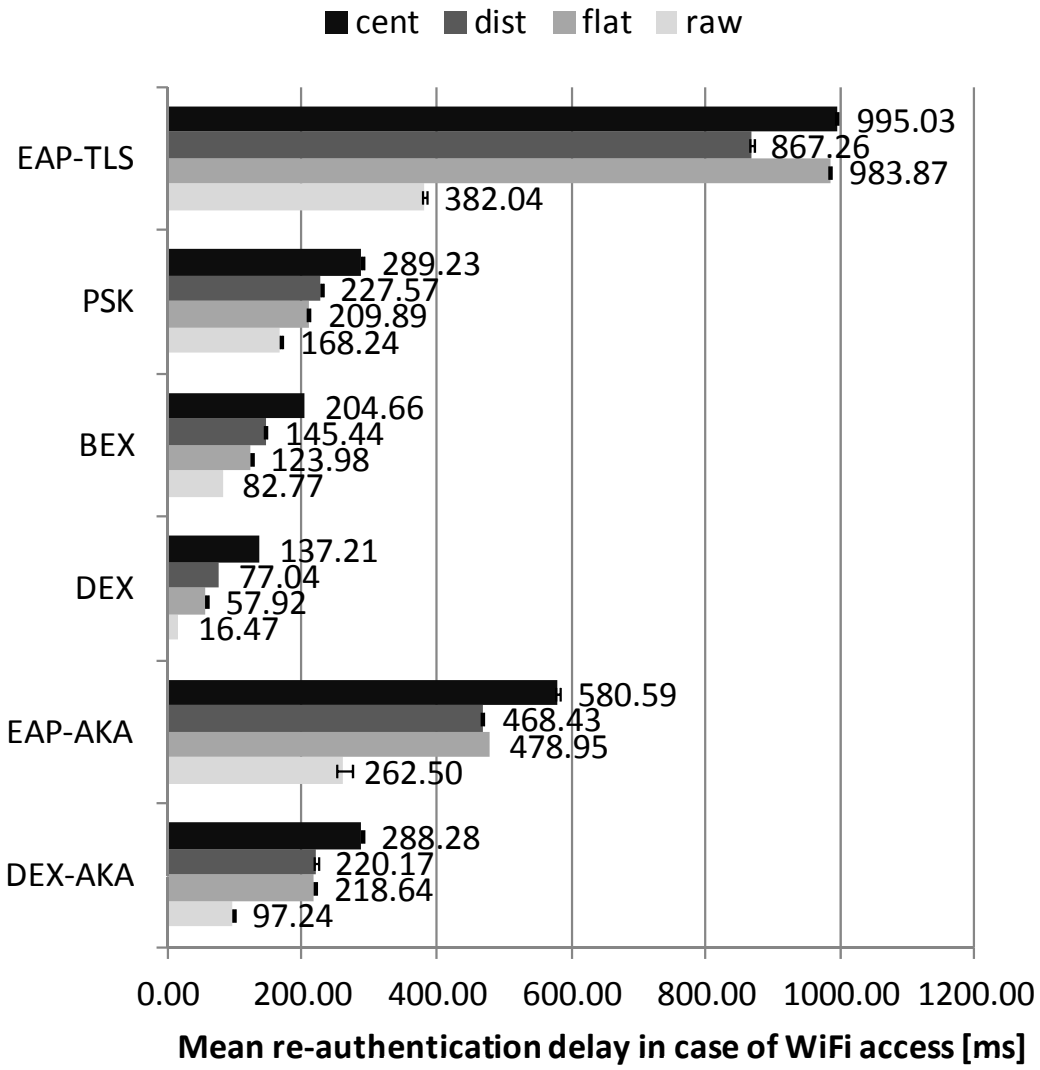
# Memory cost


AAA
GW
UE
EAP-TLS
121.2
134.6
1308.2
PSK
117.8
117.5
BEX
63.6
65.5
DEX
20.8
20.6
EAP-AKA
121.2
117.8
1142.2
DEX-AKA
24.8
24.0
0.0
200.0
400.0
600.0
800.0
1000.0
1200.0
1400.0
Peak heap and stack memory utilization of one reauthentication process [kB]

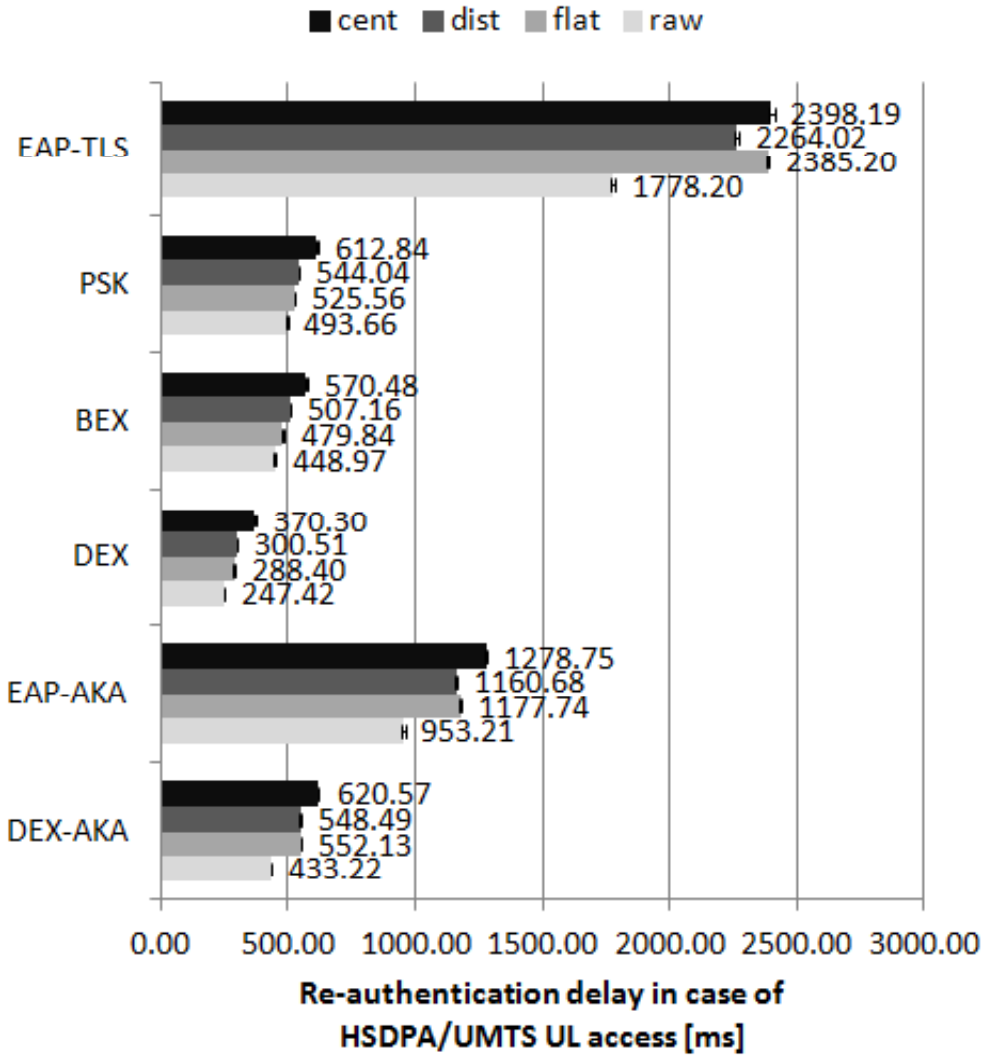
# Memory cost

- Reduction of memory utilization is significant (UE, GW: 20% DEX-AKA/EAP-AKA)
- Both in case of UEs and GWs, the memory capacity requirements are not negligible.

# Authentication delay



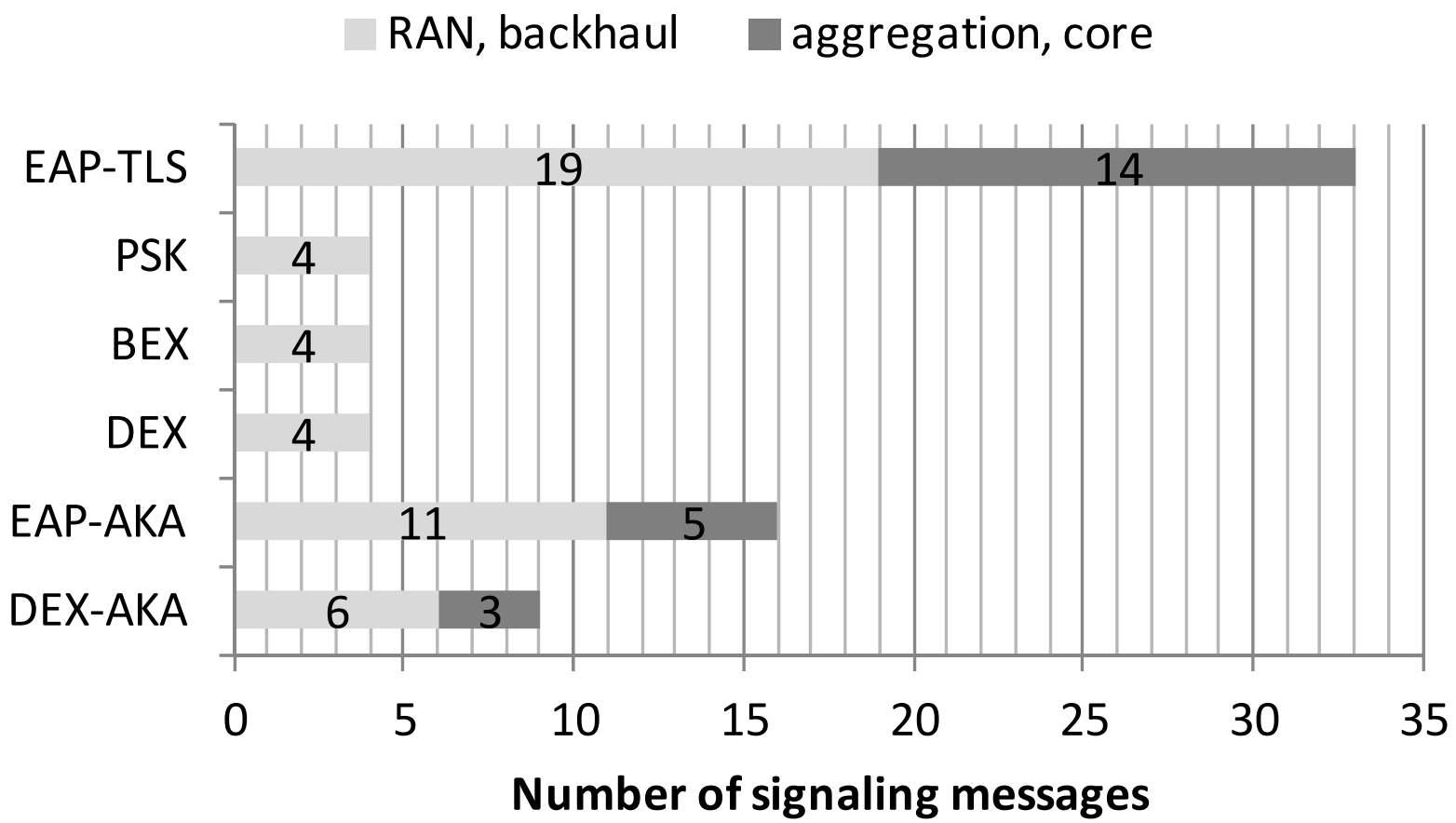
# Authentication delay



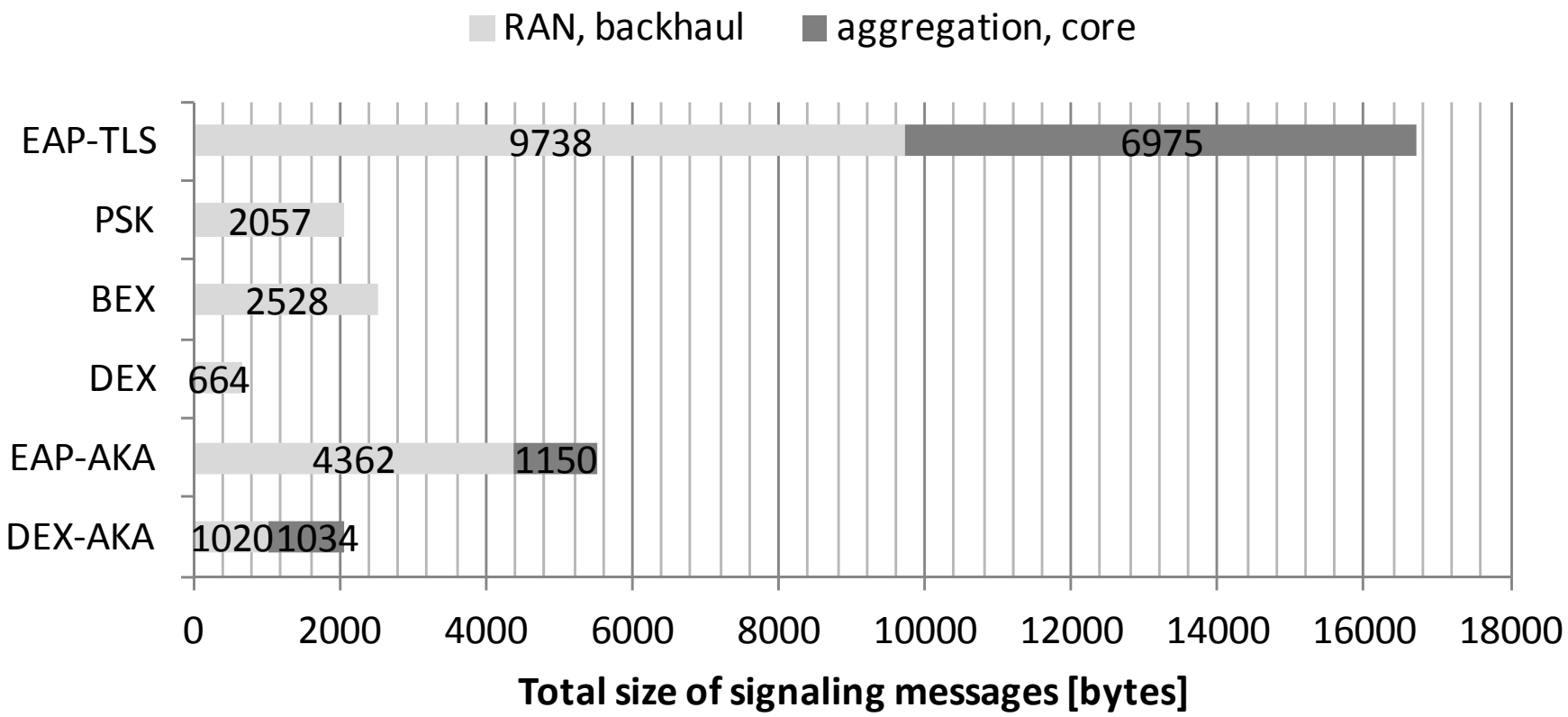
# Authentication delay

- The auhentication delay criterion is only important in case of break-before make handovers, and influences only the ongoing real-time service sessions of the user
- Break-before make handover typically happens in case of single radio handover or sudden radio link degradations.
- In case of single radio handover, re-authentication could be done proactively through the source AP. The analyzed technologies do not support this feature.
- Real-time service constraints are different for different service types.
  - TS 23.203: 50ms: real-time gaming, 100ms: conversational voice, 150ms: Live (interactive) video streaming, 300ms: Buffered video streaming (packet delay budget bw. UE and PCEF for GBR services)
- The figures show for the centralized, distributed and flat network scenario the resulting delays in case of WiFi (802.11g) and HSPA access. Note that the introduced network delays reflect worst case situations for the delay of different network parts, hence the results mean the worst case re-authentication delays. Raw scenario shows the results without added emulated delays.
- Even if DEX-AKA improves IKEv2 EAP-AKA, DEX-AKA remains only **in case of the Wi-Fi** access within some of the previously mentioned packet delay budgets (bw. 150 and 300 ms). I.e**. DEX-AKA can be used in case of GBR services with the same delay requirements as buffered video streaming**.
- The results prove that these authentication methods were not designed with fast re-authentication in mind.

# Message complexity



# Message complexity



# Message complexity

- Network link utilization should be kept low by control messages. (Reduce signaling overhead, scalable signaling)
- Both in terms of number of messages and in terms of the total size of the messages at different parts of the network , **DEX-AKA significantly overperforms EAP-AKA** (DEX-AKA:EAP-AKA proportions are 56% and 37%,respectively)

# Conclusions

- HIP DEX-AKA has significant performance gains compared to IKEv2 EAP-AKA in terms of
  - CPU load (reduction: 88% on UE, 98% on GW)
  - memory consumption (reduction 80% on UE and GW)
  - signalling (reduction: 44% in total number , 63% in total size of messages)
  - re-authentication delay:
    - WiFi access: < 300ms for HIP DEX AKA in all scenarios
    - IKEv2 EAP-AKA > 300ms, inappropriate for GBR services

# Dissemination

- Jani Pellikka, Zoltán Faigl, László Bokor, Andrei Gurtov, „Performance Evaluation of Current and Emerging Authentication Schemes for Future 3GPP Network Architectures”, *IEEE Transactions on Mobile Computing*, *submitted*

# Suitability analysis of existing and future authentication methods to EPC

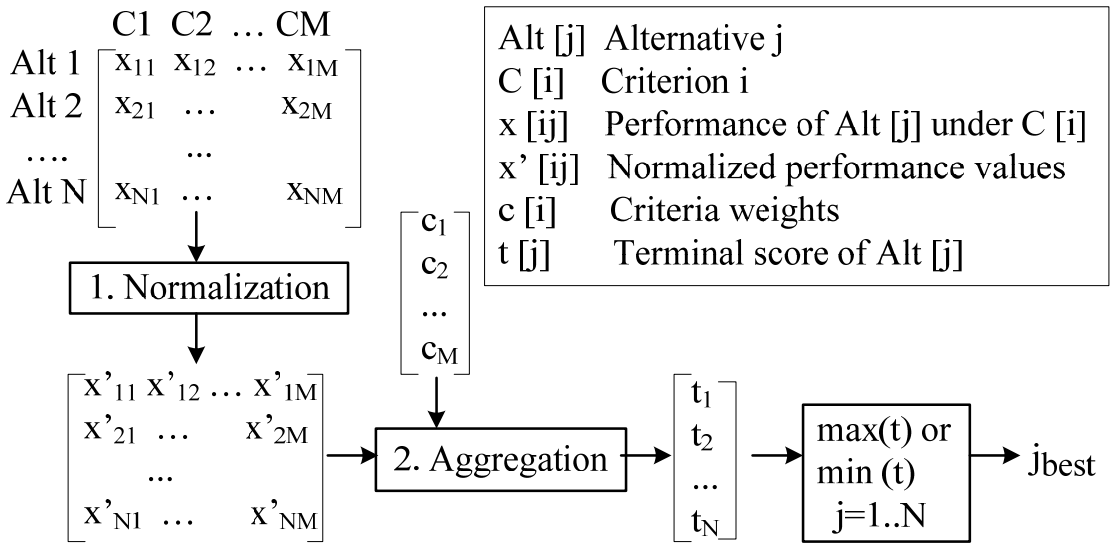
- The suitability of a new technology to an existing architecture depends on many criteria and requirements.
- The appropriate decision for the applicability of a new technology should consider all important requirements and features of the technology.

Objectives:

- Consideration of security, performance, deployment and extra-features of HIP DEX-AKA compared to other NAS technologies.
- Consider deployment options of HIP/IPsec transport in 3GPP architecture (protocol stacks)
- Focus on NAS functionality: The main objective of this validation is to compare the HIP DEX and HIP DEX-AKA authentication methods with IKEv2 EAP-AKA and other L3 authentication methods form a broader aspect, using a multi-criteria decision technique.

# Methodology

- Multi-criteria decision making (Multiplicative Analytic Hierarchy Process)



# Criteria


High security, 0.3075
0.1119
Must support mutual authentication
0.1236
Must protect the GW against DoS attack
0.1119
Must resist MiTM attacks
0.1119
Must resist replay attacks
0.0918
Must protect data traffic
0.1014
Must protect signaling traffic
0.0918
Should support perfect forward secrecy
0.0753
May support non-repudiation of attachment
0.0682
May protect host identity
0.1119
May protect user identity (IMSI)
Minimize performance cost, 0.2070
0.2231
Minimize computational cost on the
0.5782
UE
0.2444
GW
0.1775
AAA server
0.1011
Minimize memory consumption on the
0.4769
UE
0.2599
GW
0.2633
AAA server
0.4927
Minimize real-time service interruption due to full re-authentication
0.1831
Minimize the number of control packets in the
0.6529
RAN and backhaul network
0.3471
aggregation and core network
Minimize deployment cost, 0.2785
0.2447
Minimize changes in the UE
0.1455
Minimize changes in the core network
0.1098
Minimize changes in the gateway
0.2447
Minimize configuration in the UE
0.1455
Minimize configuration in the core network
0.1098
Minimize configuration in the gateway
Extra functionalities, 0.2070
0.3765
Minimize the effects of IP change (due to mobility, renumbering etc)
0.3707
May support multipath communication (dynamic registration of interfaces and IP addresses)
0.2528
May support the QoS management of signaling and data traffic

# Weight assignment

- Multiple opinion taken into account
- (7 decision makers from MIK, CWC, AALTO, FT)

| Assign differences between the *main criteria* | | | | | |
|---|---|---|---|---|---|
| | | expert 1 | expert 2 | expert 3 | expert 4 |
| importance of decision makers (P_d) | | 1 | 1 | 1 | 1 |
| **High security** | **Minimize performance cost** | -1 | 0 | -1 | 1 |
| **High security** | **Minimize deployment cost** | -2 | -2 | -2 | 0 |
| **High security** | **Support extra functionalities** | 1 | 0 | 0 | -1 |
| **index of the progression factor (i.e., γ)** | | 1 | 1 | 1 | 1 |

| Resulting criteria weights: | c_i |
|---|---|
| **High security** | **0.3075** |
| **Minimize performance cost** | **0.207** |
| **Minimize deployment cost** | **0.2785** |
| **Support extra functionalities** | **0.207** |

# Grade assignment (security)

| | DEX-AKA | EAP-AKA | DEX | BEX | PSK | EAP-TLS | Meaning of grades |
|---|---|---|---|---|---|---|---|
| Must support mutual authentication | 3 | 3 | 2 | 2 | 1 | 3 | 3: strong mutual authentication based on certificates or AKA<br>2: strong authentication of self-certifying identities, but lack of HIT verification<br>1: weak preshared key based authentication |
| Must protect the GW against DoS attack | 1 | 2 | 1 | 1 | 2 | 2 | 2: optional cookie-based DoS protection in IKEv2, GW controls the cookie distribution<br>1: puzzle-challenge based DoS protection. The attacker could have high computational capacities, hence it is hard to set the good level of puzzle. GW has less control on the access authorization than in case of cookie-distribution |
| Must resist MiTM attacks | 1 | 1 | 1 | 1 | 1 | 1 | 1: Authentication of entities, crypthoraphic binding of key material, symmetric-key based signature protection on control messages prevents MiTM attacks. |
| Must resist replay attacks | 1 | 2 | 1 | 2 | 2 | 2 | 1: weaker resistance to replay attacks in case of DEX than in case of BEX or IKEv2, the initiator (UE) does not contribute to the freshness of the messages and keys, hence replaying R1/R2 messages can lead to HIP/Ipsec state establishment in the initiator. If the initiator added a nonce to the communication and key derivation, e.g., in I2, then this attack type could be mitigated.<br>2: both peers contribute to the freshness of the communication by using random nonces from an enough large interval. |
| Must protect data traffic | 1 | 1 | 1 | 1 | 1 | 1 | 1: all methods negotiate IPsec transport, containing encryption, integrity protection, message origin authentication, anti-replay protection |
| Must protect control traffic | 1 | 1 | 1 | 1 | 1 | 1 | 1: all methods provide confidentiality, integrity protection, message origin authenticity |
| Should support perfect forward secrecy | 0 | 1 | 0 | 1 | 1 | 1 | 0: perfect forward secrecy is not provided in case of DEX, because it uses static DH key generation. If a long-term secret, such as the private key or the static DH secret established with a given peer, is compromised, previously captured confidential information can be revealed by the attacker.<br>1: perfect forward secrecy is guaranteed, due to ephemeral Diffie-Hellmann key exchange, i.e., always different DH key is negotiated. |

# Grade assignment (cont.) (deployment)

| | DEX-AKA | EAP-AKA | DEX | BEX | PSK | EAP-TLS |
|---|---|---|---|---|---|---|
| **Deployment requirements in the UE** | 1 - HIP | 0 | 1- HIP | 0 | 0 | 1 - TLS module |
| **Deployment requirements in the GW** | 2 - HIP,AAA | 0 | 1 - HIP | 1 -HIP | 0 | 0 |
| **Deployment requirements in the core network** | 2- HIPDNS,RVS | 0 | 2- HIPDNS,RVS | 2- HIPDNS,RVS | 0 | 2 - TLS module, certificate management |
| **Configuration requirements in the UE** | 0 | 0 | 1 - ACL with IDs of authorized GW's | 1 - ACL with IDs of authorized GW's | 1 - key management | 0 |
| **Configuration requirements in the GW** | 0 | 0 | 1 - ACLs with IDs of authorized GW's | 1 - ACL with IDs of authorized GW's | 1 - key management | 0 |
| **Configuration requirements in core network elements** | 0 | 0 | 0 | 0 | 0 | 0 |

$$g(P_{i,j}) = \begin{cases} 1 & P_{i,j} = 0 \\ 0 & P_{i,j} > 0 \end{cases}$$

# Grade assignment (extra functionalities)

| | DEX-AKA | EAP-AKA | DEX | BEX | PSK | EAP-TLS |
|---|---|---|---|---|---|---|
| Minimize the effects of IP change (due to mobility or renumbering) | 1 - supports using HIP mobility service | 1 - supports using MOBIKE mobilty service | 1 - supports using HIP mobility service | 1 - supports using HIP mobility service | 1 - supports using MOBIKE mobilty service | 1 - supports using MOBIKE mobilty service |
| May support multipath communication (i.e., dynamic registration of locators, multipath feature) | 2 - dynamic registration of interfaces and IP addresses supported, mHIP extension provides multipath communication | 1 - dynamic registration of interfaces and IP addresses supported | 2 - dynamic registration of interfaces and IP addresses supported, mHIP extension provides multipath communication | 2 - dynamic registration of interfaces and IP addresses supported, mHIP extension provides multipath communication | 1 - dynamic registration of interfaces and IP addresses supported | 1 - dynamic registration of interfaces and IP addresses supported |
| May support E2E QoS management for data and signaling traffic | 0 - not supported within the method, QoS policy control and enforcement by PCRF and transport network layer | 0 - not supported within the method, QoS policy control and enforcement by PCRF and transport network layer | 0 - not supported within the method, QoS policy control and enforcement by PCRF and transport network layer | 0 - not supported within the method, QoS policy control and enforcement by PCRF and transport network layer | 0 - not supported within the method, QoS policy control and enforcement by PCRF and transport network layer | 0 - not supported within the method, QoS policy control and enforcement by PCRF and transport network layer |

# Performance grade assignment

(1) Comparison to standardized constraint values :

Pj is the authentication delay of method j. The constraints are the packet delay budgets specified by TS 23.203 for different guaranteed bit-rate (GBR) service types

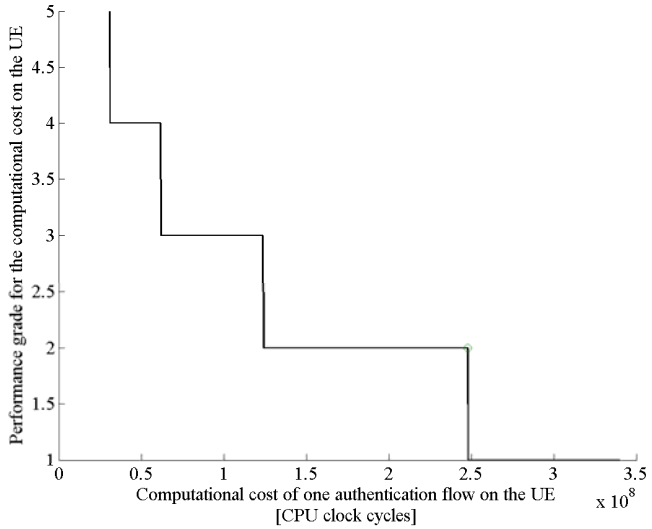
$$g(P_j) = \begin{cases} 4 & P_j \leq 50ms \\ 3 & 50ms < P_j \leq 100ms \\ 2 & 100ms < P_j \leq 150ms \\ 1 & 150ms < P_j \leq 300ms \\ 0 & P_j > 300ms \end{cases}$$

(2) Comparison to performance of current solution in 3GPP :

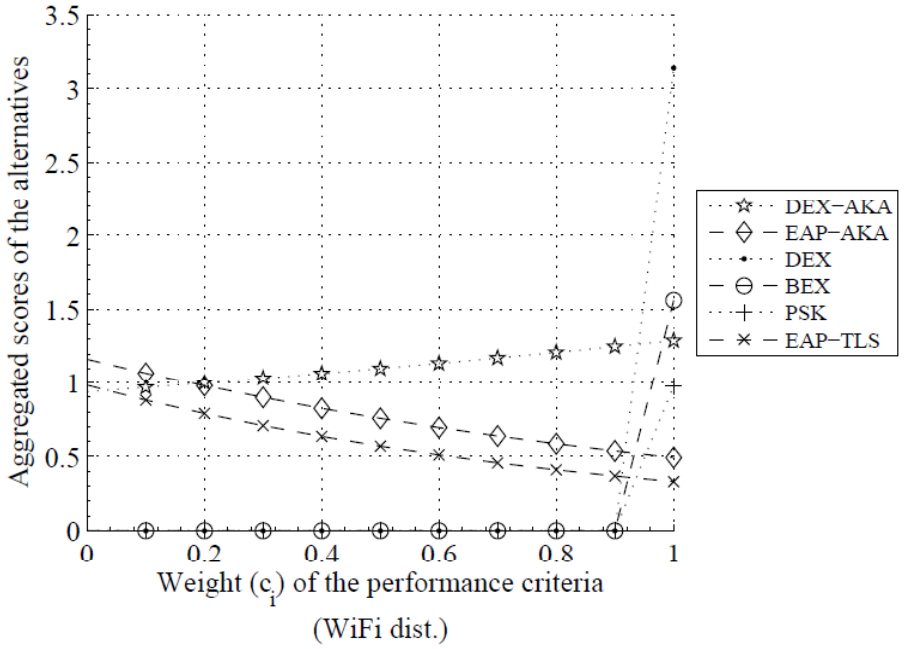
Pr (reference) is the performance of IKEv2-EAP-AKA.

| Criterion | $\gamma_i$ | $L_l$ | $L_r$ | $P_r$ |
|---|---|---|---|---|
| CPU utilization on UE | 1 | 3 | 2 | $2.48E08^{\star,\dagger}$ |
| CPU utilization on GW | 1 | 3 | 2 | $2.37E08^{\star}$ |
| CPU utilization on AAA | 1 | 3 | 2 | $4.84E06^{\star}$ |
| Mem. utilization on UE | 1 | 3 | 2 | 117.8 kB |
| Mem. utilization on GW | 1 | 3 | 2 | 121.2 kB |
| Mem. utilization on AAA | 1 | 3 | 2 | 1142 kB |
| Num. of pkts. in RAN, backhaul | 1 | 3 | 2 | 11 |
| Num. of pkts. in core | 1 | 3 | 2 | 5 |

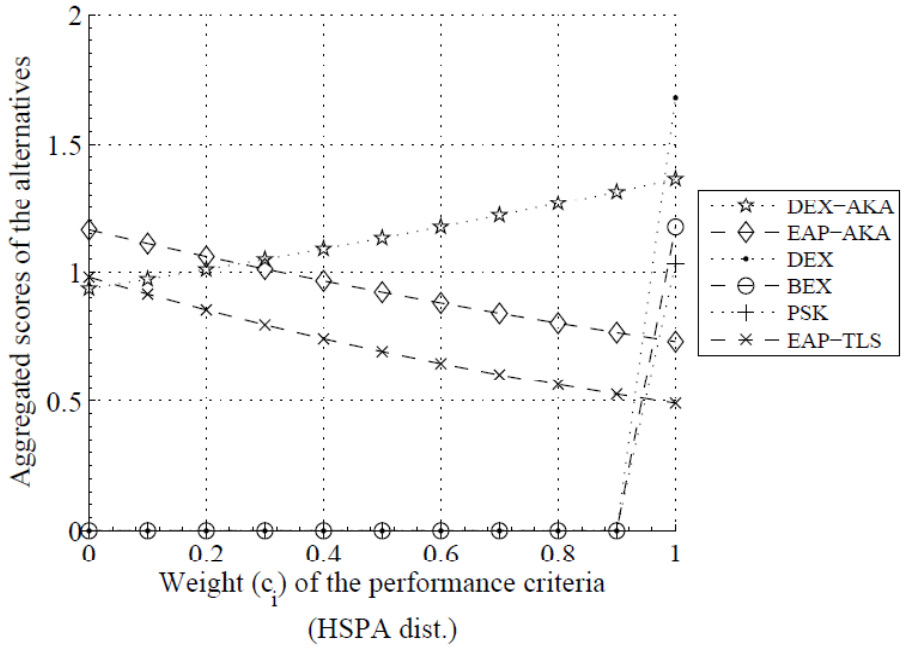
$^{\star}$ measured in terms of CPU clock cycles,



# Sensitivity analysis (weight of performance criteria)

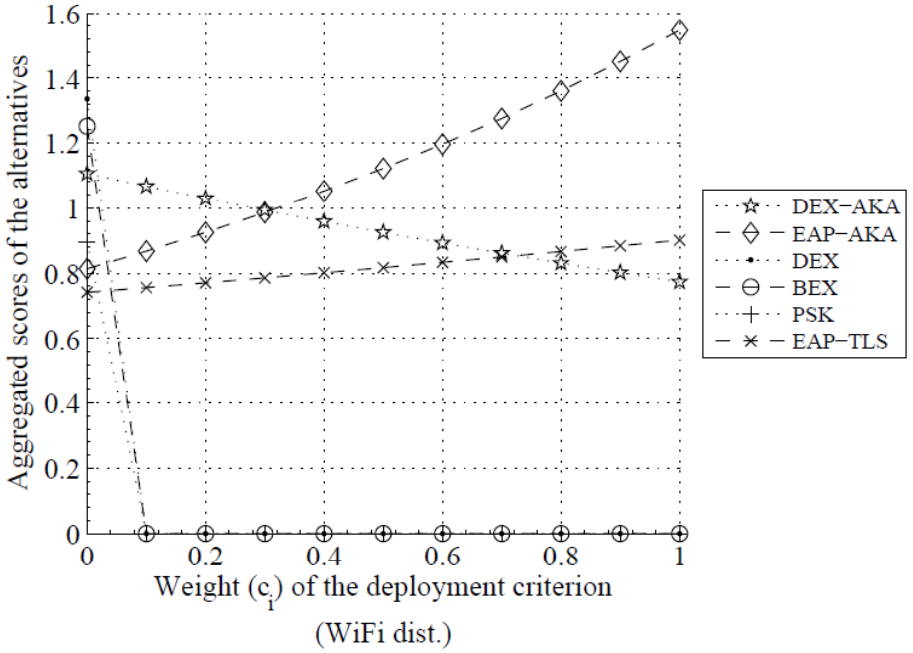



(WiFi dist.)

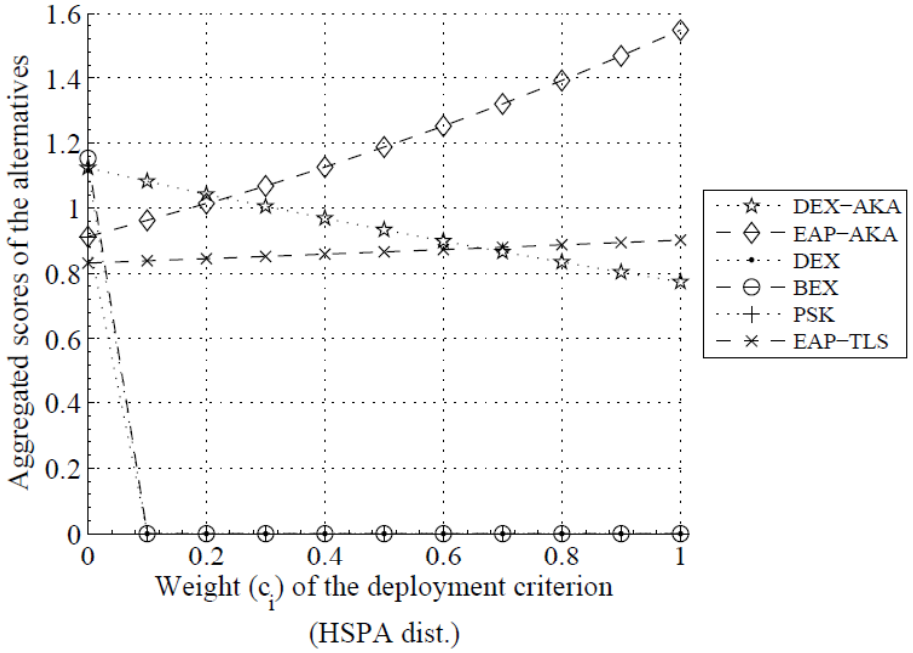



(HSPA dist.)

# Sensitivity analysis (cont.) (weight of deployment criteria)

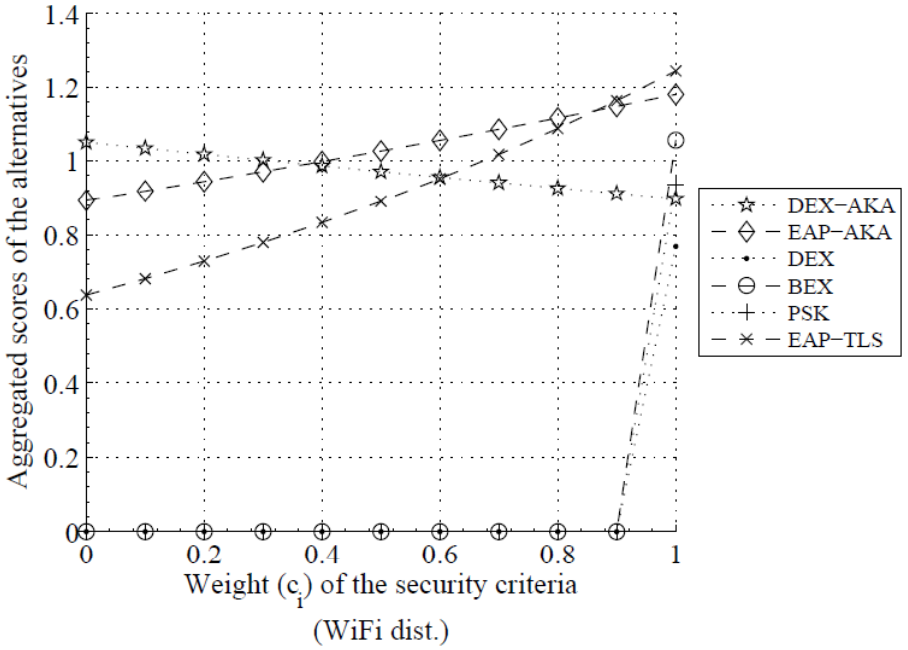


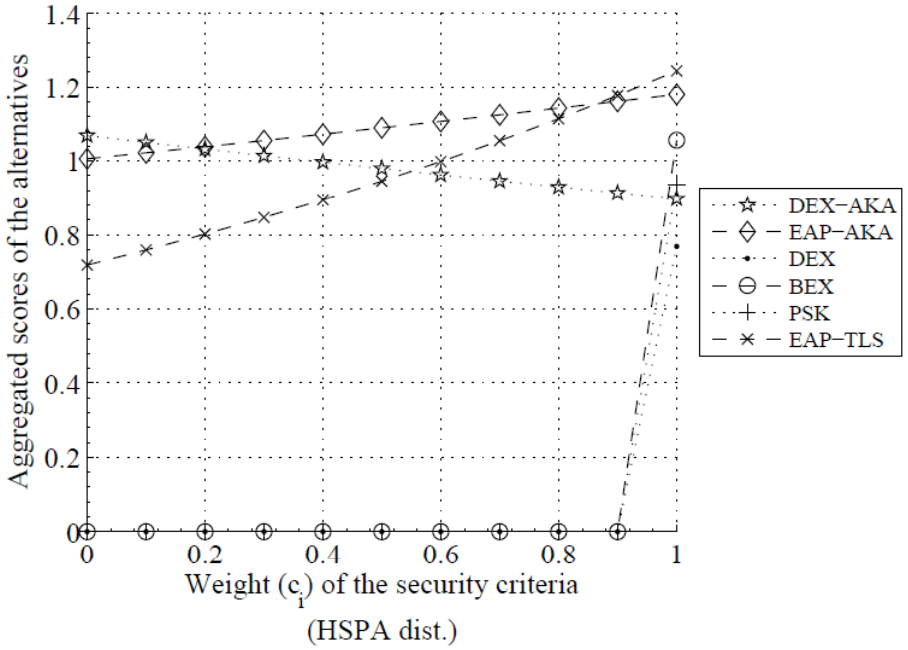
(WiFi dist.)



(HSPA dist.)

# Sensitivity analysis (cont.) (weight of security criteria)



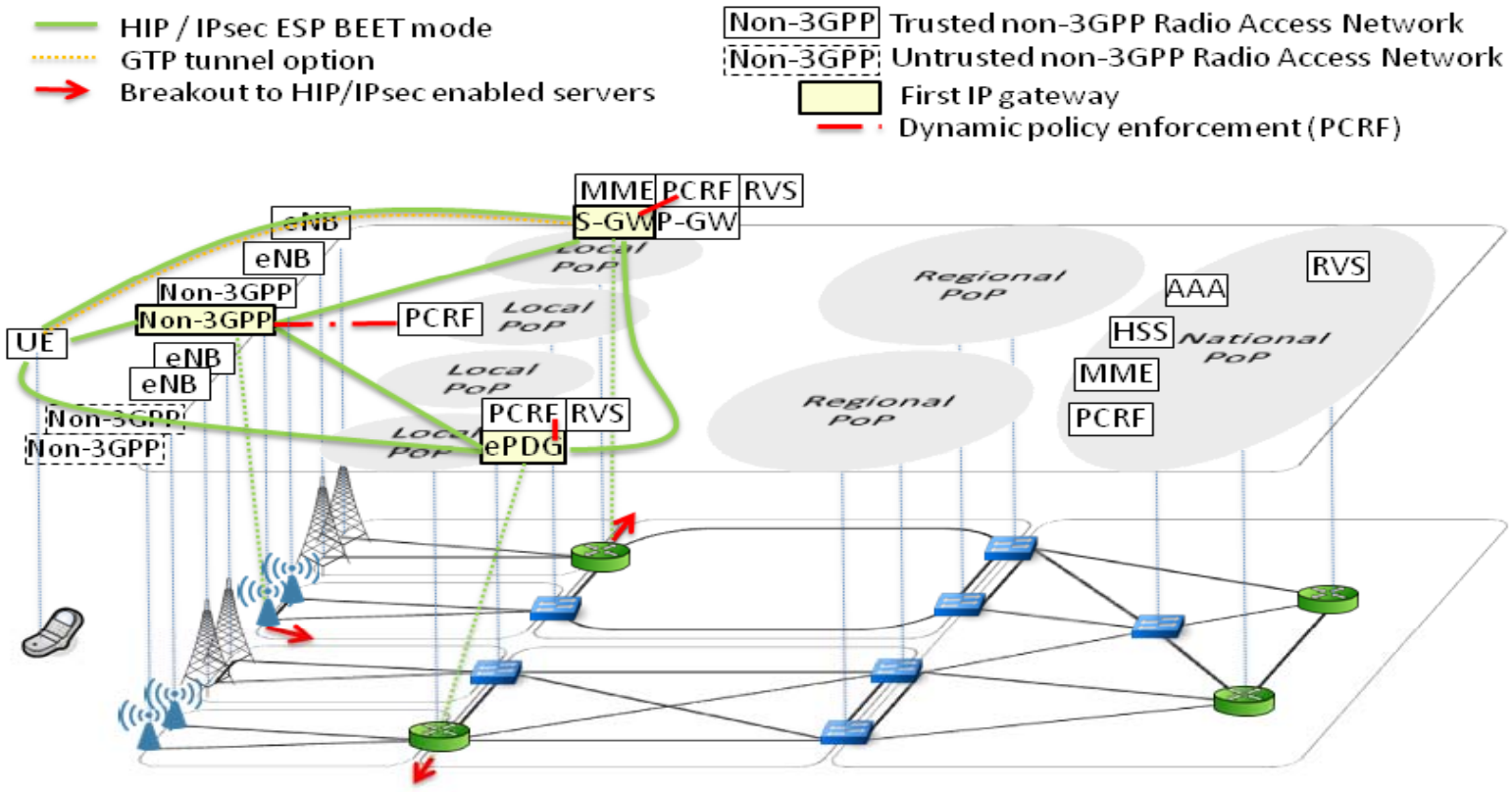



# Conclusions

- We analyzed the exact trade-offs and overall ranking of the authentication methods under criteria weights defined by seven experts in the field of mobile telecommunications.
- With sensitivity analysis we analyzed the robustness of the results.
- It seems that the criteria weights obtained based on the opinions are near to weight allocation points where the ordering of the methods change.

- The results show that HIP DEX-AKA authentication has competitive features compared to the other methods, such as the IKEv2 EAP-AKA currently recommended in untrusted non-3GPP IP accesses.
- HIP DEX-AKA achieves significant gains in terms of performance, and supports such functionalities that makes favorable its use in mobile networks where the access network is frequently changed.
- On the other hand it has slightly weaker security than IKEv2 EAP-AKA and high deployment cost.
- Hence, its usage is recommended in use cases requiring highly resource-constrained UEs and uniformly secure communication within mobile networks such as the 3GPP EPC.

# Distributed/flat architecture



# HIP/IPsec based tunneling

Deployment in two phases.

1) The first phase would include a parallel use of DSMIP/PMIP/GTP-based tunneling and the HIP-based UFA (UFA-HIP) .
   - intra-GW handover and tunnel management handled by the existing IP tunneling services.
   - inter-GW handovers between P-GW, S-GW, ePDG, BNGs managed by the UFA-HIP solution by deploying the UFA-HIP technology in the P-GWs.

2) In the second phase
   - protocol architecture could be further simplified
   - standardized tunneling options would be replaced HIP/IPsec tunneling both between GWs and between UEs and GWs.
   - For 3GPP-Access GTP tunneling would be still required between the first GW and the eNodeB, but not required in case of non-3GPP accesses.

# HIP/IPsec based tunneling

- Benefits
  - uniform security over any access network,
  - service continuity in case of inter-GW handovers,
  - support for legacy applications
  - support of coexistence of IPv4 and IPv6 network segments, transparent for UEs and applications becomes possible due to HIP.
  - the support of seamless inter- and intra-GW handovers due to UFA-HIP (from the 2nd phase)
- Drawback:
  - Deployment requires change in the UE and the network
  - IPsec overhead

# Dissemination

- Zoltán Faigl, Jani Pellikka, László Bokor, Andrei Gurtov, „Suitability Analysis of Existing and New Authentication Methods for Future 3GPP Evolved Packet Core”, *Elsevier Computer Networks*, *submitted*

# Next steps

- Multiple IPsec connection for the same HIP host association for QoS mapping
- Defining cross-layer paging procedures for optimized lookup of sleeping mobile nodes
- NEMO route optimization for nested scenarios

# Virtualization of the technology

- Currently, RVS and HIP-enabled DNS service are assumed for the provision of naming and addressing
  - It would be interesting to analyze distributed naming and addressing (HIP Hi3)
  - Multiple IPsec SAs should be supported by HIP for different traffic classes.
- The software-defined transport network layer should enforce QoS policies.
  - Invesitage where is the exact place of microscopic and macroscopic traffic management
  - Investigate priorization of decision policies in different layers of the network (RAN, transport, mobile service, application)
  - This is a more generic research topic

# Thank you for your attention!
# Any questions?