Smarter technology for all

6G Security Study Work Task Input(s)

Lenovo, Motorola Mobility

01 August 2025

Smarter technology for all

Lenovo

6G Security Architecture

6G Security Architecture

- Justification
  - Security architecture and key hierarchy should be unified, simple and comprehensive to support any UE to network secure interaction.
  - e.g., AS, NAS, application services, data collection, data provisioning, sensitive service/network slice cryptographic isolation (e.g., AMF reallocation in case of lack of N14 kind of scenarios) etc.,
  - Avoid complex and too many security establishment procedures.

- 6G Security Study 'Work Task on Security architecture and key hierarchy'
  - Study and identify the potential connections and scenarios which falls in the scope of 6G E2E system security.
  - Study and define a holistic 6G Security architecture that covers all possible scenarios as applicable e.g., including but not limited to different PLMN, NPN and PNINPN deployments.
  - Study and define a common 6G key hierarchy to support any required UE to Network connection/communication Security as applicable (e.g., AS, NAS, application services, data collection, data provisioning, sensitive service/network slice cryptographic isolation (e.g., AMF reallocation in case of lack of N14 kind of scenarios) etc.,)
  - Study and define the security establishment procedures (key refresh as applicable) in alignment with the defined 6G Key hierarchy

Smarter technology for all

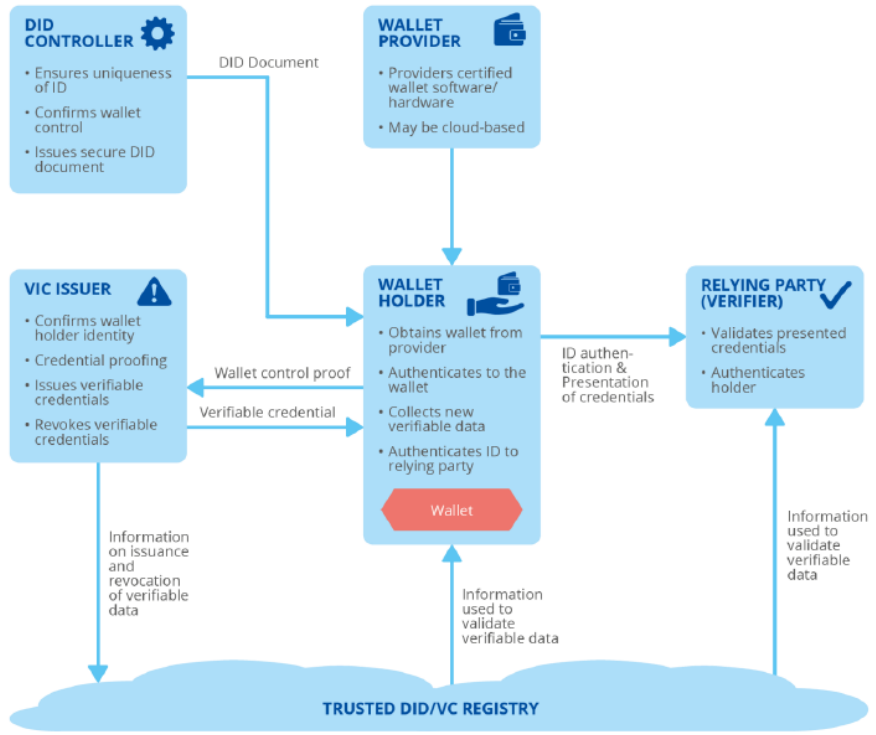
Digital / Decentralized Identification & Authentication for 6G Systems

Lenovo

DID Content Overview

1. Overview of Decentralized/Digital identification (DID) work happened so far (e.g., W3C DID, ETSI PDL)
   - Refer:
     - W3C DID (https://www.w3.org/TR/did-1.1/)
     - EU eIDAS2 Unified digital ID framework and related Self Sovereign Identity initiatives!
     - ENISA, 'Digital Identity, Leveraging the Self-Sovereign Identity (SSI) Concept'
     - ETSI PDL-0023, 'PDL service enablers for Decentralized Identification and Trust Management'
     - ETSI PDL-0027, 'Permissioned Distributed Ledger (PDL); Self-Sovereign Identity (SSI) in telecom networks'
2. Rationale - How can 3GPP network and services access security benefit from using DID and Verifiable Credentials (VC) concepts?
3. Current 3GPP Status: SA1 requirement level directions towards DID concepts
4. Proposed SA3 6G Study Work Tasks

Figure 6: SSI Actors and their responsibilities



Source: ENISA, 'Digital Identity', Leveraging the Self-Sovereign Identity (SSI) Concept to Build Trust

Rationale: How 3GPP network and services can benefit from using DID and Verifiable Credentials (VC) concepts

- Limitations with the existing ID/Credentials Management
  - Single point of failure
  - Complexity and delay with initial trust establishment

- Benefits - Decentralized Identity and VCs
  - Resistant to single point of failure and ID/credentials lock-in situations.
  - Flexible ID/Credentials generation and usage
  - Decentralized nature ensures non-repudiation, tamper resistance
  - Combination of DID and Selective disclosure property of VC ensures privacy preservation

- UE
  - Simplify Onboarding network access Scenarios
  - MNO as ID service provider for 3rd party service(s)
  - Simplify KYC for MNO subscription activation*

- RAN Node/function
  - Prevent single point failure with ID/credentials management
  - Avoid complexity with trust establishment across different security domains
  - Achieve flexible ID and credentials management for RAN authentication

- Core NF/AF
  - Prevent single point failure with id/credentials management
  - Avoid complexity with trust establishment across different security domains
  - Achieve flexible ID and credentials management for NF/AF authentication

Reference*

GSMA, "Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid".

Europa Futurium, 'eIDAS Supported Self-Sovereign Identity'.

Current 3GPP Status: 6G SA1 requirement level directions towards DID concepts [UE]

- **6G TR 22.870_031**
  - 5.5.4 6G security requirements
    - Security as a service for digital identity based on SIM identity and authentication:
      - Operators can leverage the SIM identity as the root ID of user to associate the following digital identity of the digital human, robots, etc., and enable users to seamlessly access various services and resources of the Internet.
      - Accordingly, the operators can associate the digital human with the digital Identity and the final root of ID of the SIM.
      - Furthermore, SIM-based self-sovereign identity for authentication and associated attributes for authorization can be used to provide flexible access control of identity access control as well.
    - [PR 5.5.4.2-7] The 6G system shall enable operators using SIM as trust anchor to provide identity and authentication service to the 3rd parties.
    - [PR 5.5.4.2-8] The 6G system shall support the verification for the association between the SIM identity and the digital identity of the different digital avatars.
      - Editor's Note: Digital avatar is FFS.
    - [PR 5.5.4.2-9] The 6G system shall authorize the required services of the digital identity of the digital avatars of users and revoke the digital identity if needed.
      - Editor's Note: Digital avatar is FFS.
  - 9.11 Use case on digital identity management for digital asset container
    - [PR 9.11.6-1] Subject to operator policy and user consent, the 6G system shall support verification of digital identities issued by a third party.
      - Editor's Note: This requirement is FFS.

Current 3GPP Status: SA1 requirement level directions towards DID concepts [Network/Core]

- **6G TR 22.870_021**
  - 5.3.1 Network Security for 6G
    - it is important to decrease the administrative and operational burden for establishing security within and between 3GPP networks. As seen today, many operators struggle with the bilateral administration of security to enable interconnection and roaming with other operators.
    - Therefore, a decentralized, yet common approach for exchanging security keys and authentication/authorization credentials is needed.
    - [PR 5.3.1.2-1] The 6G network shall provide security mechanisms for secure access to elements of the core network of the 6G system and secure communication on all 3GPP defined interfaces of the core network of the 6G system.
    - [PR 5.3.1.2-2] The 6G network shall support establishment of secure communication between elements of the network while protecting network related information (e.g. network element identities, topology) from disclosure to unauthorized parties.
    - [PR 5.3.1.2-3] The 6G network shall provide security mechanisms that enable the network operator to ensure there are no unintended changes of the elements of the 6G network.
  - 5.3.4 6G security requirements
    - **Efficient trust establishment and secure communication in inter-PLMNs and intra-PLMNs:**
    - Frequent cross-domain authentication brings about network latency and management cost, as well as threats of single point of failure. What's more, it is difficult to establish a common root of trust for cross domain communication.
    - The issue has been identified prominently in the inter-PLMN case, where operators face problems of managing the large scale of CAs in roaming scenarios. Thus, an efficient and decentralized manner of establishing trust in inter-PLMN connection is needed.
    - [PR 5.3.4.2-1] The 6G system shall provide efficient mechanisms to support authentication and secure communication in inter-PLMN and intra-PLMN networks.

Proposed Work Tasks

- 6G Security Study ‘Work Task on Digital Identification and authentication’
  - Study and Identify the security use case(s) in 6G System which can benefit from Digital identity-based authentication, selective data disclosure and credentials control.
  - Study how the Digital Identification and trust establishment framework can be supported for the 6G System for UE Authentication and Network Authentication.
  - Study how digital identification and authentication can be procedurally supported for the identified security use cases.

Smarter technology for all

AI for 6G E2E Trust and Security

Lenovo

AI for 6G E2E Trust and Security

- Justification
  - Massive connectivity expected in 6G Systems*, UE to network connection may experience connection abuse/attack attempts**.
  - Connection abuse & security threats may also occur in RAN and Core network too
  - Leverage AI and other applicable means (if any) for threat detection.
  - Enable security/trust evaluation-driven access control security for 6G E2E Systems.

- 6G Security Study Work Task on Enablers for 6G E2E Trusted and Secure Connections.
  - Study the feasible methods to identify security risk/threats at 6G UE, RAN and Core.
  - Study and define resilient access control security approaches to protect the 6G assets (UE, RAN, Core as applicable) in case of potential security breach/threat detection.

References
*6G - Statistics & Facts, 'https://www.statista.com/topics/7163/6g/#topicOverview'.
**Telecom Sector - Cyber Risk, 2025, 'https://kpmg.com/in/en/blogs/2025/02/telecom-sector-cyber-risk.html'.

Smarter technology for all

Security for AI in 6GS

Lenovo

Security for AI in 6GS

- Justification
  - AI/ML plays a major role in 6G Systems
    - For network automation, AI model training/inference assistance service to 3rd party/subscribers etc. as in TR 22.870.
  - Suitable security approaches need to be in place to handle security vulnerabilities in various AI/ML operations and its lifecycle.
  - In-depth security vulnerability analysis of all AI/ML operations (e.g., Training, inference, model storage, model transit) should be considered while developing AI/ML Security aspects.
- 6G Security Study Work Task on 'Secure AI/ML'
  - Study the potential security vulnerabilities of AI/ML operations.
    - NOTE: For reference, can consider the AI/ML operations and 6G System usage scenarios described in TR 22.870.
  - Study and define solutions to secure AI/ML operations in 6GS against the identified security vulnerabilities.

Smarter technology for all

Data Exposure Security (Network / Application Level)

Lenovo

Data Exposure Security

- Data exposure (network and user data exposure) can happen in the 6G network / application layer as applicable
  - TR 22.870 – Example requirements on UE related data exposure
    - Clause 5.5.5 Usecase on enhanced exposure
      - [PR 5.5.5.2-1] Subject to regulation, operator(s) policy and user consent, the 6G network shall support procedure(s) to expose aggregated (non-sensitive/anonymized/non-personally identifiable) information related to UEs, served by the network, e.g. number of UEs in a geographical location, their mobility pattern, application usage trends, from the network to authorized 3rd parties without exposing UE identities.
    - Clause 5.5.7 Use Case on privacy protection of data exposure
      - [PR 5.5.7.3-1] Subject to operator policy and regulatory requirements, the 6G system shall support privacy protection for any information exposure to a 3rd party.
      - [PR 5.5.7.3-2] Subject to national or regional regulatory requirement, the 6G system shall provide user privacy protection, location privacy, identity protection for UEs accessing 6G network for services (e.g. communication, sensing, AI inferencing), and for the corresponding information exposure to an authorized 3rd party.
      - [PR 5.5.7.3-3] The 6G system shall be able to protect UE's subscriber identities from attacks.
    - Clause 11.18 Use case on network-requested execution of service functions in connected devices
      - [PR 11.18.6-1]: Subject to operator policy, regulatory requirements and user consent, the 6G network shall provide suitable APIs to allow authorized third parties to collect data from UEs (e.g. connected vehicles) that are located in a specific area and are capable of collecting data upon network request.
      - [PR 11.18.6-2]: Subject to operator policy, regulatory requirements and user consent, the 6G network shall enable UEs (e.g. connected vehicles) to indicate whether they can collect data upon network request.
  - Examples for Network related data exposure: TR 22.780
    - 6.1 Use case on optimizing 6G infrastructure utilization via resource exposure in 6G
    - 5.8.3 Use case on supporting energy control at slice level
- Privacy protection, confidentiality, authorized data exposure & user consent (as applicable) are critical aspect of data exposure security.

- 6G Security Study Work Task on Data Exposure Privacy and Security
  - Study and define the potential security requirements of UE data exposure
  - Study and define the potential security requirements of Network data exposure
    - NOTE1: Study and list the scenarios from TR 22.780 which requires network level data exposure and list the scenarios which requires application-level data exposure. This information can be used as baseline scenario to define the respective security solution.
  - For Network level/layer data exposure, study and define the security mechanisms to enable unified data exposure security.
  - For Application level/layer data exposure, study and define the security mechanisms to enable unified data exposure security.

Smarter technology for all

Data Privacy and User Consent (Network / Application Level)

Lenovo

Data Privacy & User Consent

- Lesson learnt from 5G:
  - Ambiguous – 3GPP/out of 3GPP scope, definitions, redundant terms and so on.
  - At Network Level: Different features related to user consent for 3GPP features/privacy profiles for UE location info usage/exposure.
    - Subscriber related User Consent Check aspects were defined in TS 33.501 to be used when required for 3GPP features/services. The collection and format aspect is out of 3GPP scope.
    - For LMF, different privacy classes and Location privacy indications (LPI) (Location for UE is disallowed or allowed) are defined in TS 23.273. LPI can be provided and updated by UE using NA NAS message (or) by AFs via NEF.
  - At application Level: CAPIF feature defines Resource owner authorization.
    - i.e., The permission provided by RO to allow the API invoker to access the RO's resource via the northbound API.
- Most of the use case (e.g., around 41UC) in 6G TR 22.870 largely bound to the user consent.
  - As user consent tied upto user privacy, data protection and regulatory requirments, Utmost Care should be taken in SA3 WG to address the following aspects:
    - What aspects of user consent are out of scope of 3GPP and what is in scope of 3GPP (if any).
    - Right and unfied definition of user consent.
    - List of scenarios goverened by user consent.
    - Is there additional concepts like privacy profile/resource owner authorization/permission aspects needed? If yes how to hormonize additional aspects related to user consent with unified terms, definitions and procesures?

- 6G Security Study Work Task on Data Privacy & User Consent
  - Study and identify the potential scenarios (both 3GPP features and exposure to 3rd party) which requires data privacy and user consent.
  - Case 1: Study the security solution to enable data privacy (and govern user consent) as applicable in case of 3GPP features.
  - Case 2: Study the security solution to enable data privacy (and govern user consent) as applicable in case of UE data exposure to 3rd party.
  - NOTE: There may be a unified or dedicated solution for the above two cases. Study the pros and cons of both.

Smarter technology for all

Lenovo

thanks.