Security Conference

FRONT-END ACCESS MANAGEMENT

Presented by: Andras Vilmos

17/10/2023

Key Considerations

- **The need**
  - Cybercrime needs to be fought with new technologies
- **The concept**
  - Secure elements in smart phones are underutilized
- **The opportunity**
  - The SIM is potentially opening up
    - SAM (Secure Applications for Mobile) by GSMA
    - OMAPI (Open Mobile API)
    - EUDIW (EU Digital Identity Wallet)
- **The know-how and expertise**
  - Consumer centric secure element management
  - Chip card expertise
  - Secure service implementations

Key Technology Trends

User needs
- Privacy
- Greater control
- Independence
- Convenience

New design approaches
- Distributed architectures
- Reduced communication
- Robust security
- Resources at the edge
- Tokenisation

New services emerge
- Web3.0
- Decentralized Identity (DID)
- Verified Credentials (VC)
- eIDAS 2* – EU Digital ID wallet (EUDIW)

Identity and Access Management

User identification – authentication (OIDC)

Confirms users are, who they claim they are

User authorisation (OAuth)

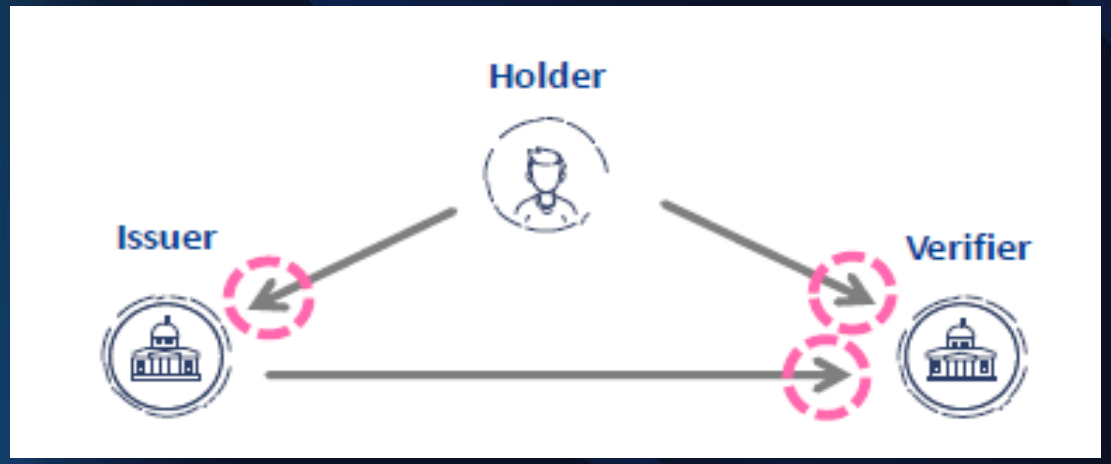
Allows users access to protected resources

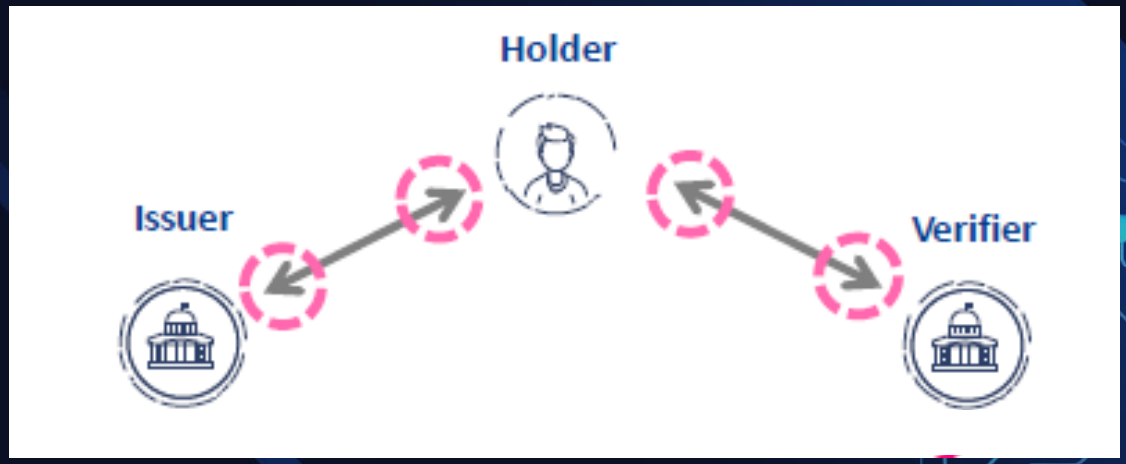
Transformation of OIDC

OpenID

Limitations of OpenID Connect
- Allows user profiling by Identity Provider
- Constrained to related Verifiers
- Users (Holders) have limited control

Advantageous specifics of OID4VC
- Control over when and what to disclose
- Portability
- Privacy
- Selective disclosure of attributes
- Simpler technical implementation
- Distributed system – decentralized





Figures from EBSI

Differences between authentication and authorisation

Authentication vs Authorisation

- Identities are stable – may never change
- Identities are portable – may be used in different situations, environments
- Identity information are for repetitious use – the same information is reusable
- Identities comprise multiple static attributes (credentials) – selective disclosure may be used for presentation

- Access rights are dynamic – may frequently change
- Access rights are purpose bound– may only be used in specific relationships
- Authorisation are unique and for specific occasions – credentials should not be reusable
- Access rights may be non-specific – constrains may be used instead of distinct values

Different specifics call for different technologies.
What works for authentication may not work for authorisation.

Transformation From OAuth to FEAM (OAuth4VC ???)

Novelty of FEAM

A new form of using the secure element

Extension of FIDO*

In FIDO chipcards are used for user identification.

In FEAM they are also used for transaction authorisation.
FEAM uses the secure element not only for storing digital keys but also to store access credentials.

* https://fidoalliance.org/

A new place of generating the signed tokens

Decentralization of OAUTH

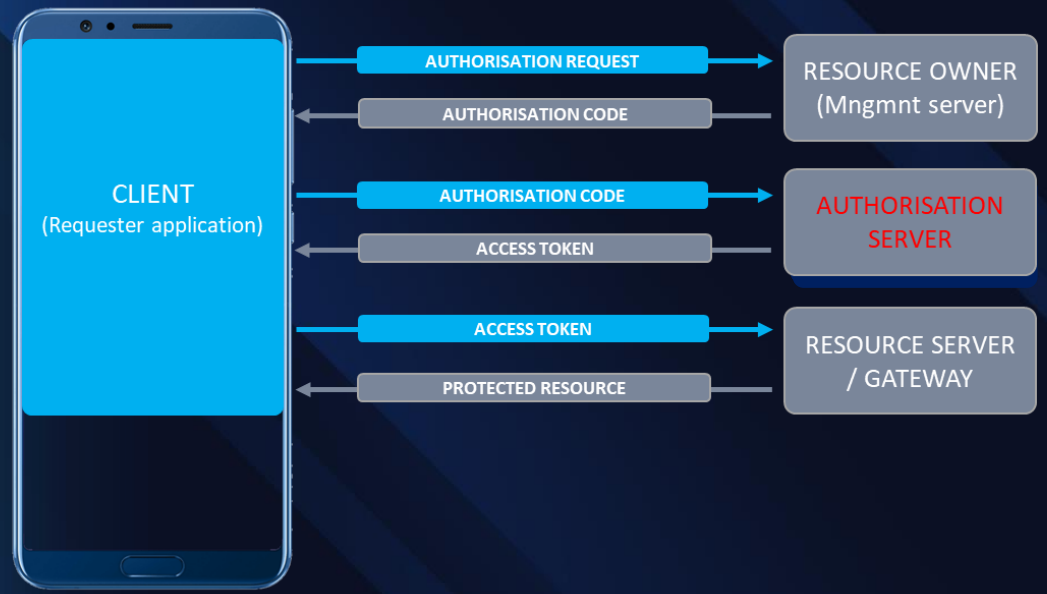
In OAUTH2.0 each transaction needs server communication.

In FEAM the server is only connected when user privileges (access credentials) are refreshed.
FEAM performs authorisation on the user's secure element and not in a server.

** https://oauth.net/

How OAuth works

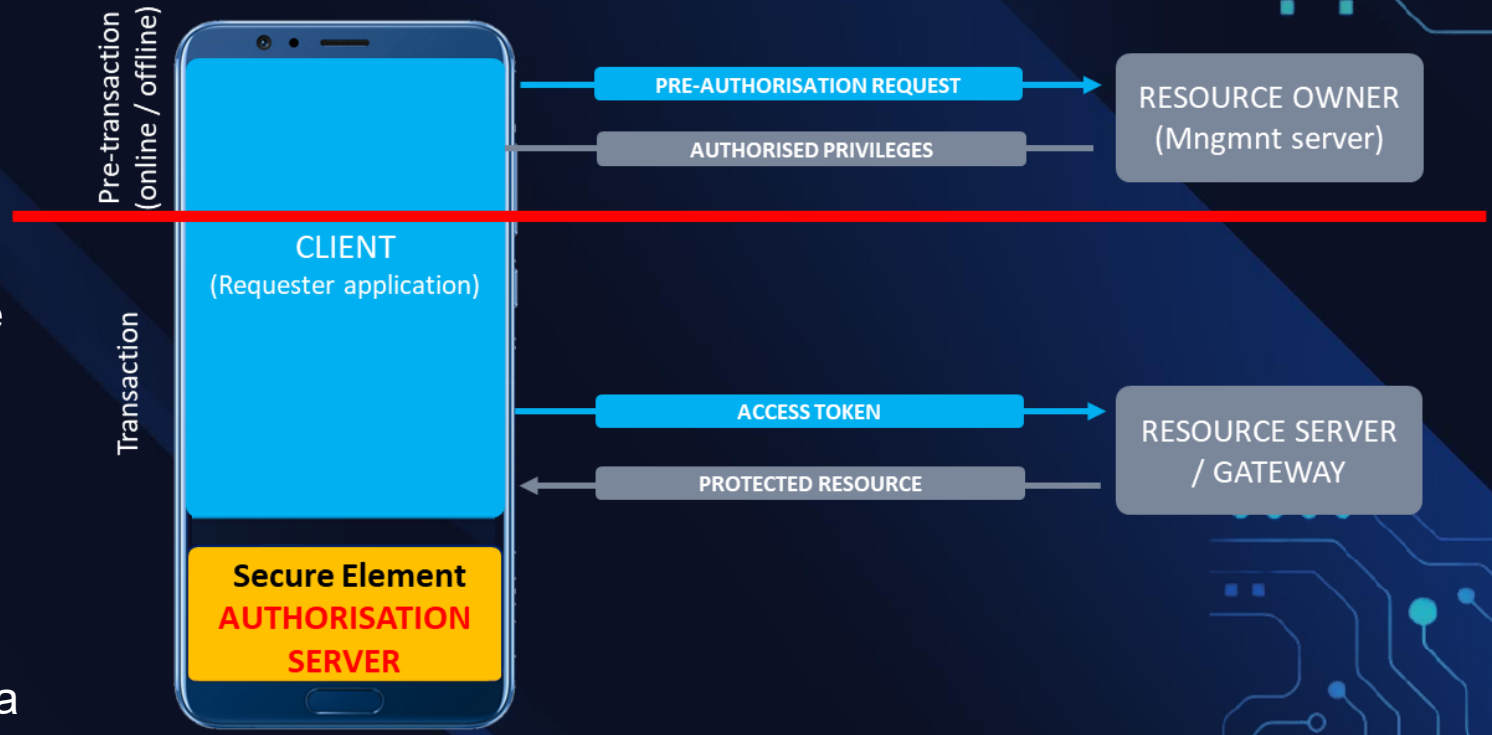
OAUTH - Authorisation Code Flow



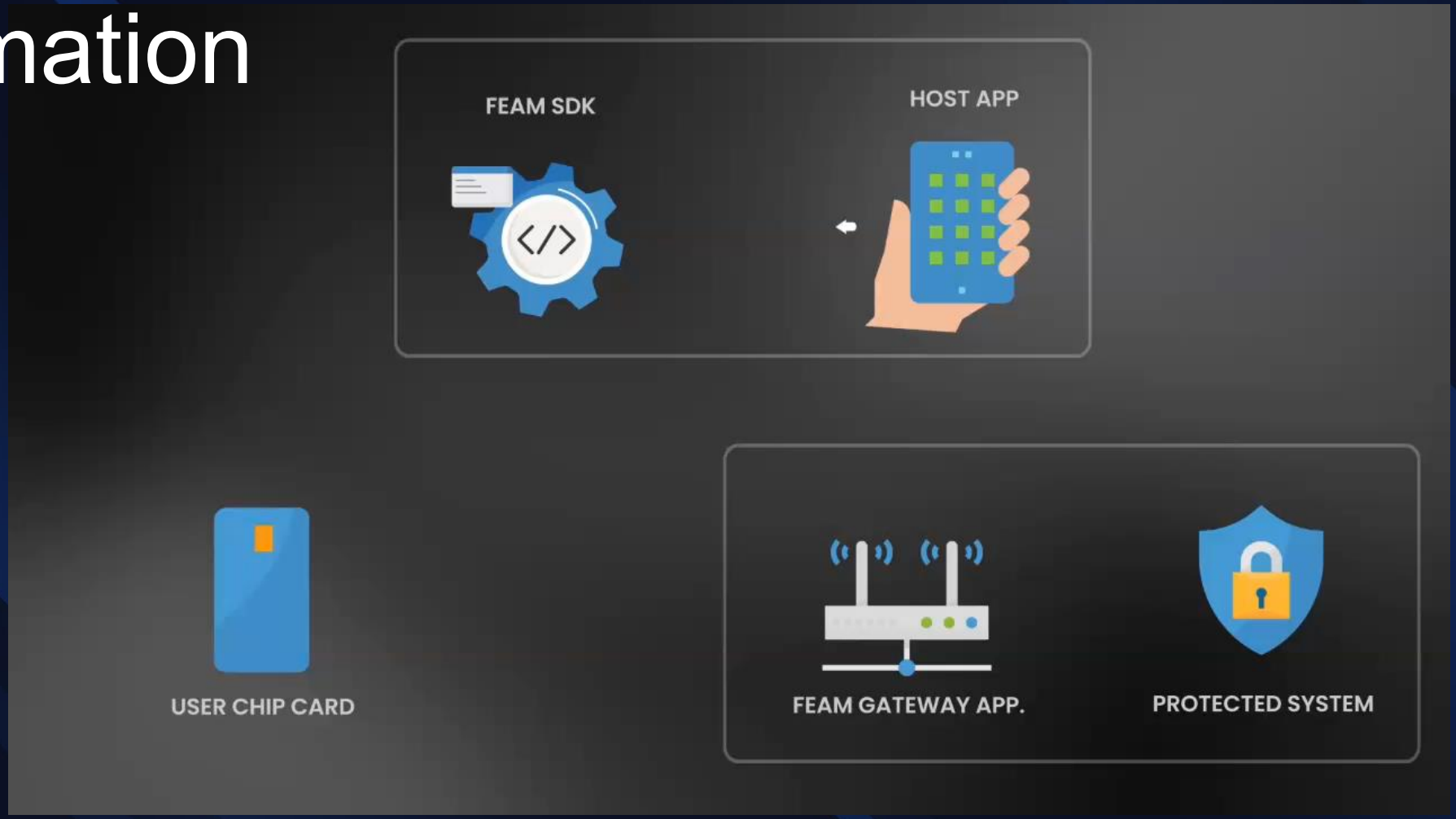
- Request a code from an Identity provider
- Exchange the code for a signed token (JWT)
- Present the token at the point of access

Moving to the FEAM Model

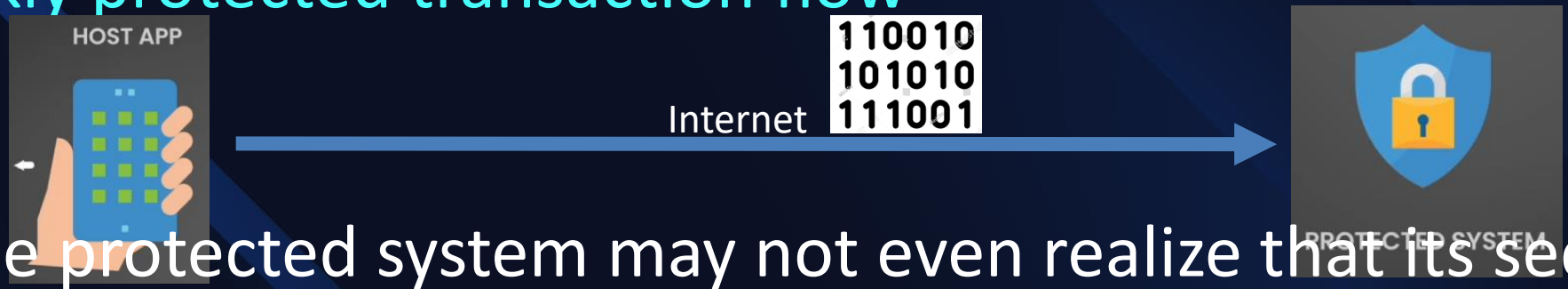
- FEAM introduces secure element (chip card) on the user side
- Authorisation server function is moved to the user secure element
- Authorisation request is replaced by issuance of privileges to secure element
- Privileges (CREDENTIALS) are securely stored in the secure element
- No server communication is used to perform a transaction



Animation

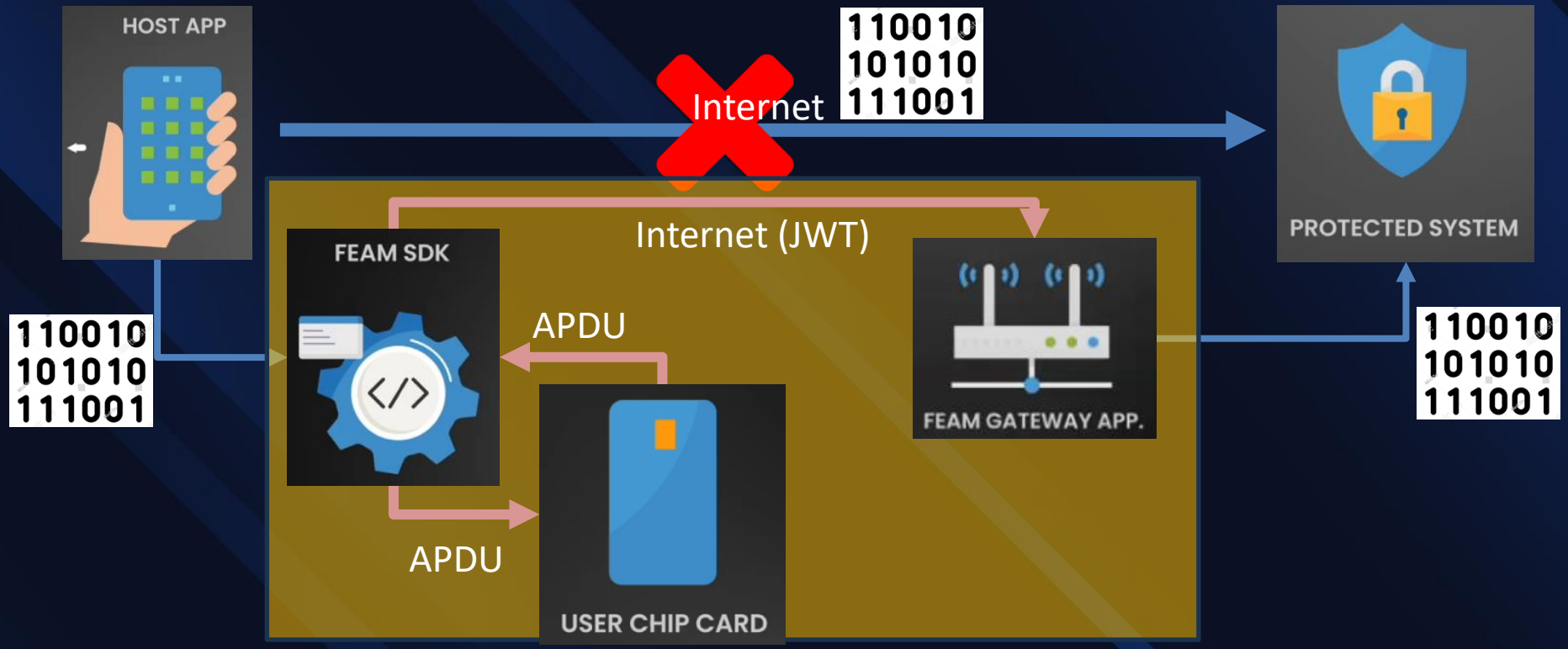

FEAM SDK
HOST APP
USER CHIP CARD
FEAM GATEWAY APP.
PROTECTED SYSTEM

Weakly protected transaction flow



The protected system may not even realize that its security environment has been substantially improved!

FEAM transaction flow



FEAM Security Features

- Use of smart card – highest level protection
- 2+ factor authentication
- Use of PKI
- End-to-end communication encryption
- No data on online server (optional)
- Full user control
- User anonymity (optional)
- Session based authentication and authorisation
- Just in time privileges
- Real-time revocation/blocking of privileges
- Auditable delegation of rights
- Removal of single point of access failure (optional)

Specifics of FEAM

User friendliness

- Transparent security technology
- Hidden use of chip card
- Diverse client devices
- Over the air management capability

Efficiency

- Quick deployment and integration
- Automated operation
- Good scalability
- Full remote management

Flexibility

- Cloud based or on- premise operation
- Online and off-line transactions
- Diverse operating domains
- Modular architecture

FEAM is a highly secure, decentralised, user friendly, and robust IAM system securing architectures from smart homes to complex IIoT operations.

FEAM could be the centerpiece of Zero Trust Security Architectures.

FEAM vs. the State of the Art (SoA)

- Using a secure element (chip card), PKI and multi-factor authentication for all transactions, FEAM is more secure than most other technologies
- FEAM may not store any sensitive user information on internet facing servers
  - SoA performs authentication and/or authorisation online over the internet
- FEAM avoids the single point of access failure by its delegated operating structure
  - SoA needs to connect to a single authorisation point even for decentralized services
- FEAM minimizes communication overhead by avoiding remote server authorisation
  - SoA needs to call a remote server for each user authentication and transaction authorisation
- FEAM executes off-line and online transactions with equal security level
  - SoA cannot authorize fully off-line transactions without some security compromise
- FEAM can prevent user profiling, if necessary, still maintaining the highest protection
  - SSO services may monitor all activities of their users which is a privacy threat

Transaction Scenarios

Multi-cloud Access

High Security Architectures

Offline Transactions

Device Onboarding

Takeaways

- FEAM USES THE SECURE ELEMENT (chip card) for authenticating the user, authorizing the transactions as well as generating and signing the access token. This approach minimizes the communication overhead, removes single point of access errors, and facilitates the same security for completely off-line transactions as for online ones.
- THE SOLUTION ALSO SATISFIES ALL ZERO TRUST REQUIREMENTS including session-based authorisation, least privilege and just in time privilege principles, and generates extensive audit logs. In addition, the technology also makes a huge step to increase privacy as no central third party can monitor when and where the privileges have been used.
- FEAM COULD ALSO BE USED WITH ALREADY DEPLOYED ARCHITECTURES as the technology follows the OAUTH standard. This means that already from the start it could have a sizeable acceptance environment.

SAFEPAY

THANK YOU

safepaysys.com

vilmos@safepaysys.com