ENSURING IDENTITY PRIVACY AND MITIGATING SECURITY RISKS IN CLOUD SERVICES

Presentation by Jan Lindquist

Mobile Application Security Core – Product Manager and ISO/CEN Privacy and Security Standards Expert

GOLD STANDARD (ENCRYPTION-BASED) SECURITY

We craft solutions that protect the most sensitive personal data from unauthorized access and meet strict compliance regulations.
Our expertise spans four product lines:

KEY MANAGEMENT

MOBILE APP SECURITY

DIGITAL IDENTITIES & SIGNATURES

PAYMENTS

The art of cryptographic security requires us to be at the cutting edge of data and computer science.
Every year, we invest millions into Research and Development to keep you and your customers safe.

30+ YEARS OF INNOVATION

30+ BLUE CHIP CLIENTS

30+ COUNTRIES SERVED

20+ INDUSTRIES PROTECTED

OVERVIEW

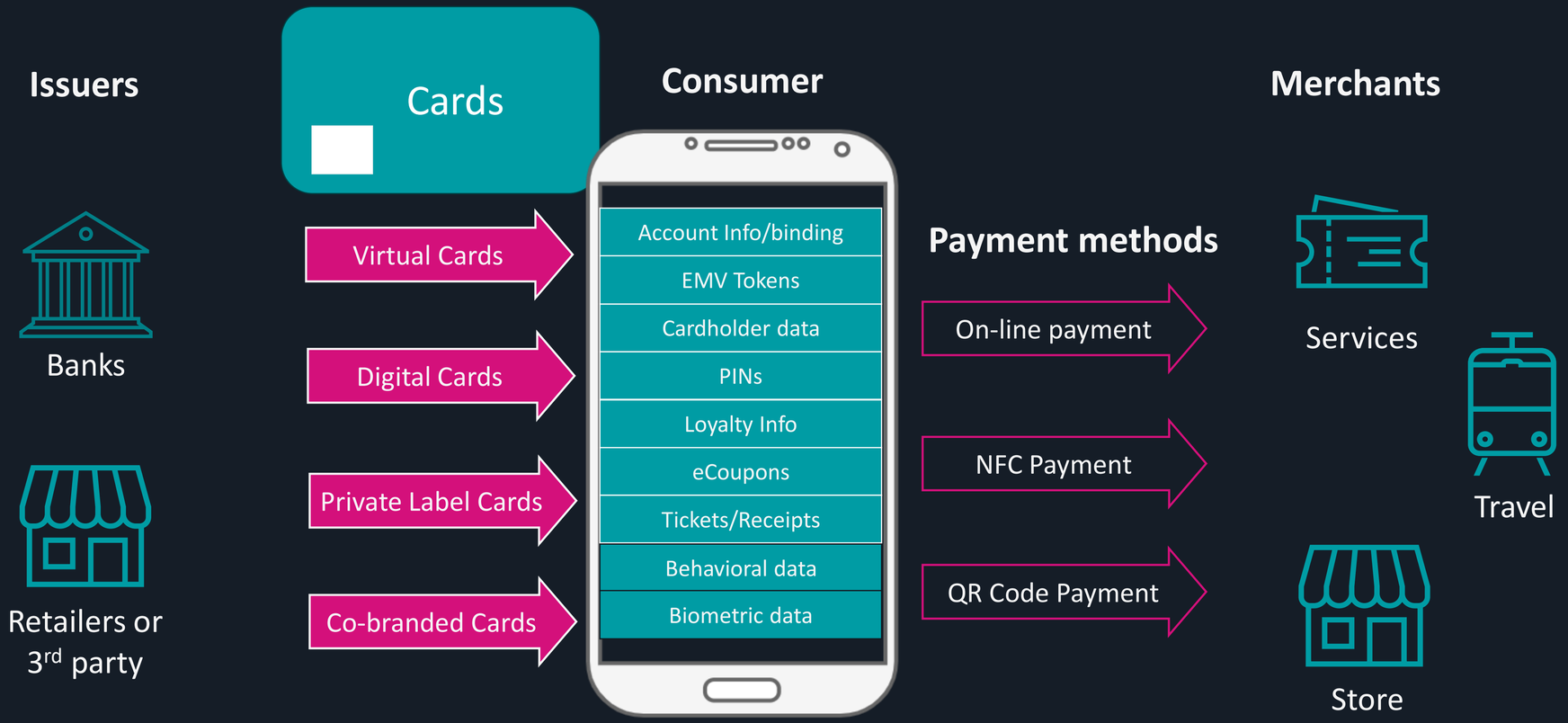
Goal 1: Role of the mobile towards secure cloud service (use cases)

Goal 2: Transparency with processing notice

Goal 3: Overview NIST and EU Security Regulation and Assessment

Goal 4: Understanding security threats and mitigation

FINANCIAL WALLET APP SERVICES



Wallets types:
- Closed
- Semi-opened
- Opened

WALLET APP SERVICES

CRYPTOMATHIC

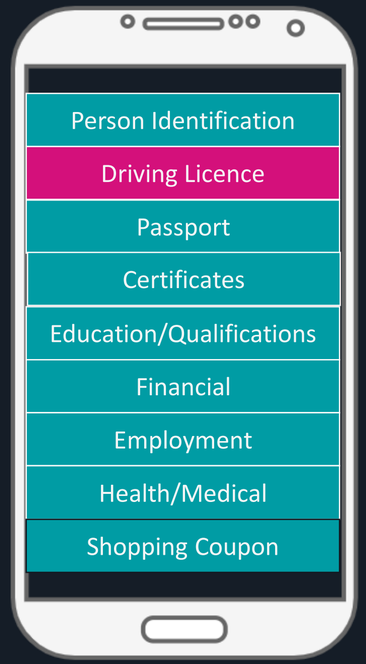
Qualified Providers (Issuers)

Certificates

Person Id Data

Attestations

Consumer



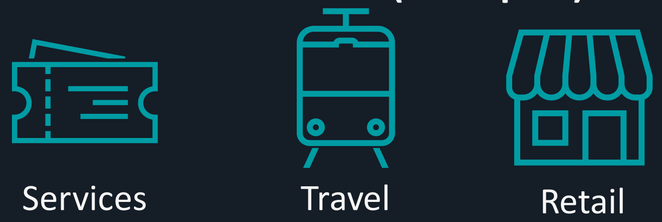
Online Access

Consent

Selective Disclosure

Relying parties (examples)

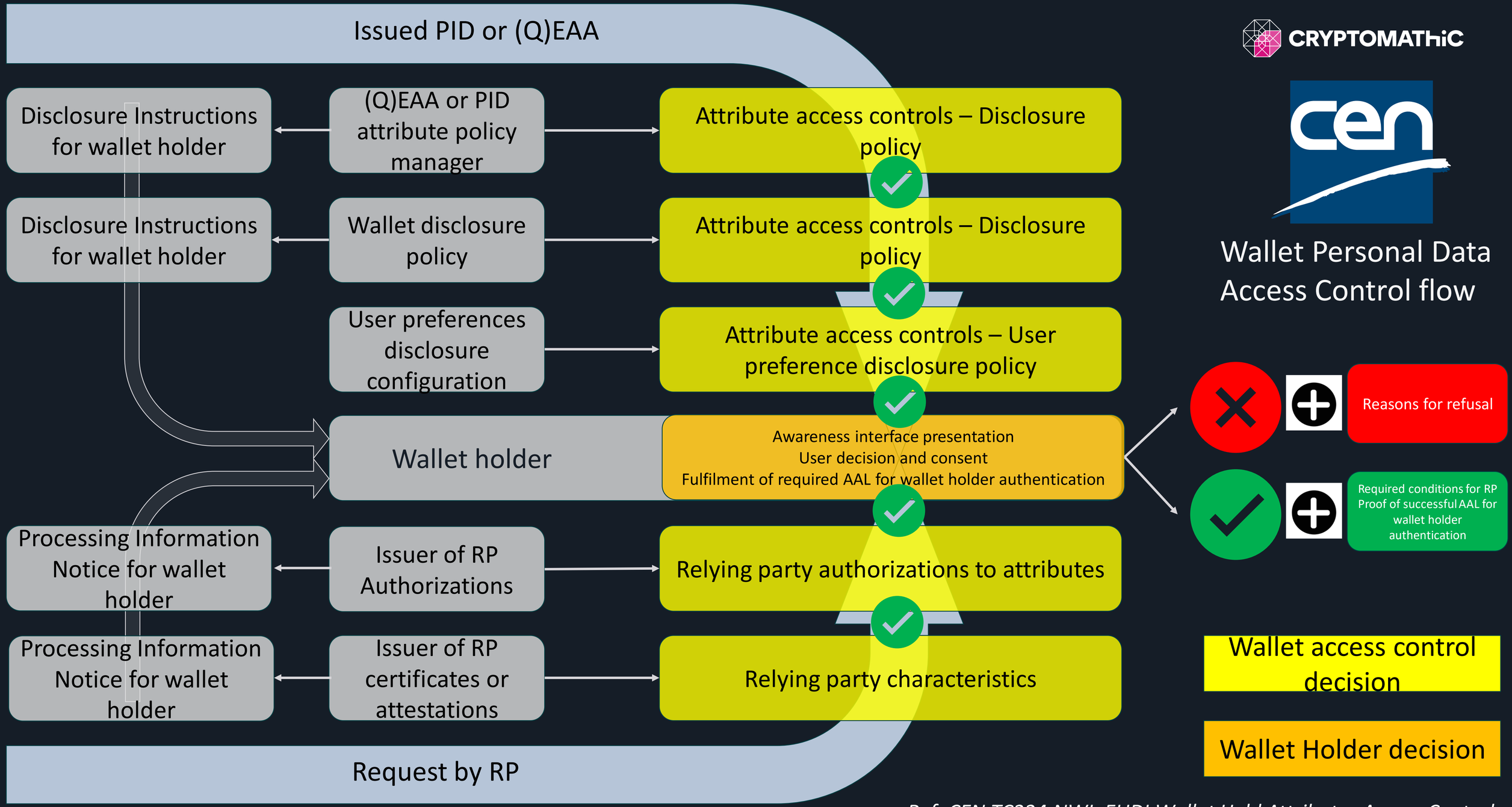
Other Providers (Examples)



Other Relying Parties (Examples)

EU FUNDED LARGE SCALE PROJECTS

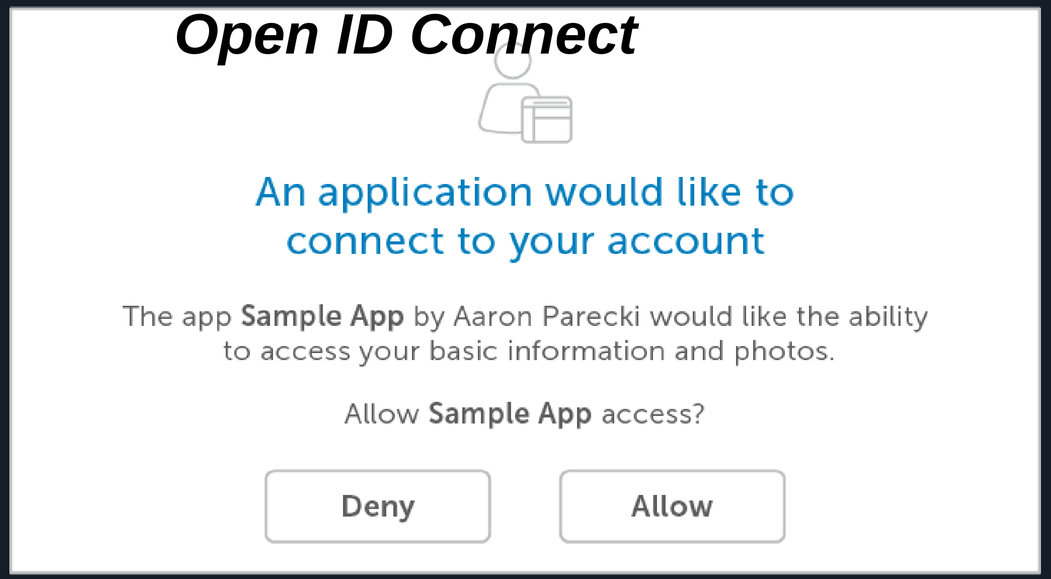
1. POTENTIAL – Pilots for European Digital Identity Wallet Consortium
   - Access to government services
   - Opening of a bank account
   - Registration for a SIM card
   - Mobile driving licence
   - eSignatures
   - ePrescriptions
2. EWC – EU Digital Identity Wallet Consortium
   - The storage and display of digital travel credentials
   - The organisation of digital wallets
   - The organisation of payments
3. NOBID – Nordic-Baltic eID Wallet Consortium
   - Authorisation of payments for products and services
4. DC4EU – Digital Credentials for Europe Consortium
   - Educational sector and the social security domain.


Issued PID or (Q)EAA
Disclosure Instructions for wallet holder
(Q)EAA or PID attribute policy manager
Attribute access controls – Disclosure policy
Disclosure Instructions for wallet holder
Wallet disclosure policy
Attribute access controls – Disclosure policy
User preferences disclosure configuration
Attribute access controls – User preference disclosure policy
Wallet holder
Awareness interface presentation
User decision and consent
Fulfilment of required AAL for wallet holder authentication
Reasons for refusal
Required conditions for RP
Proof of successful AAL for wallet holder authentication
Processing Information Notice for wallet holder
Issuer of RP Authorizations
Relying party authorizations to attributes
Processing Information Notice for wallet holder
Issuer of RP certificates or attestations
Relying party characteristics
Request by RP
CRYPTOMATHiC
Wallet Personal Data Access Control flow
Wallet access control decision
Wallet Holder decision
Ref: CEN TC224 NWI: EUDI Wallet Held Attributes Access Control

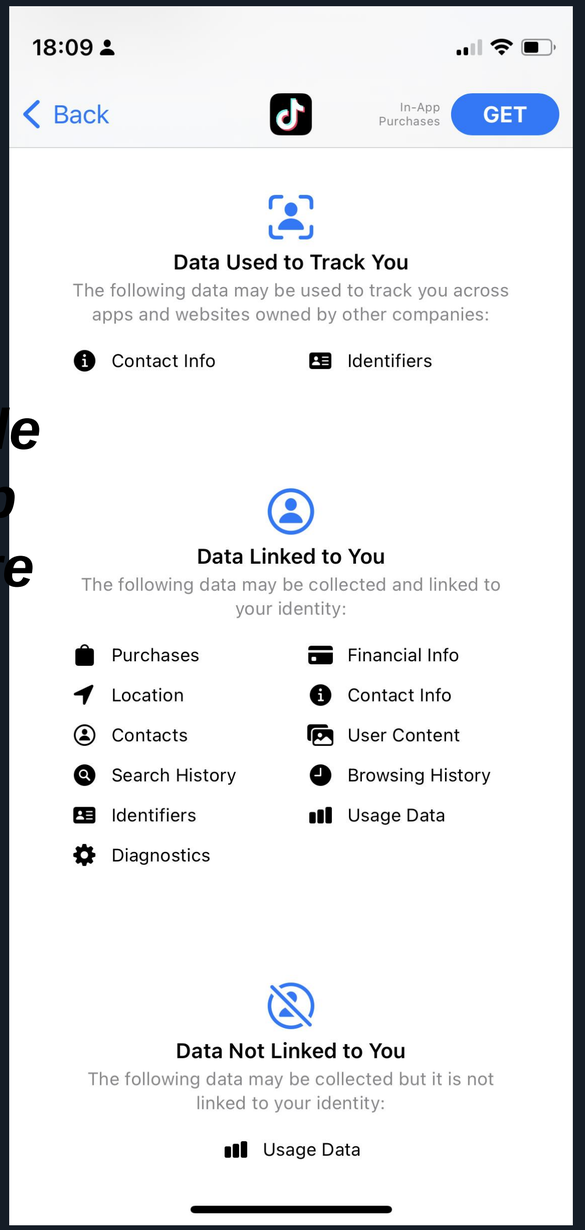
PRIVACY NOTICES CHALLENGES

CRYPTOMATHIC

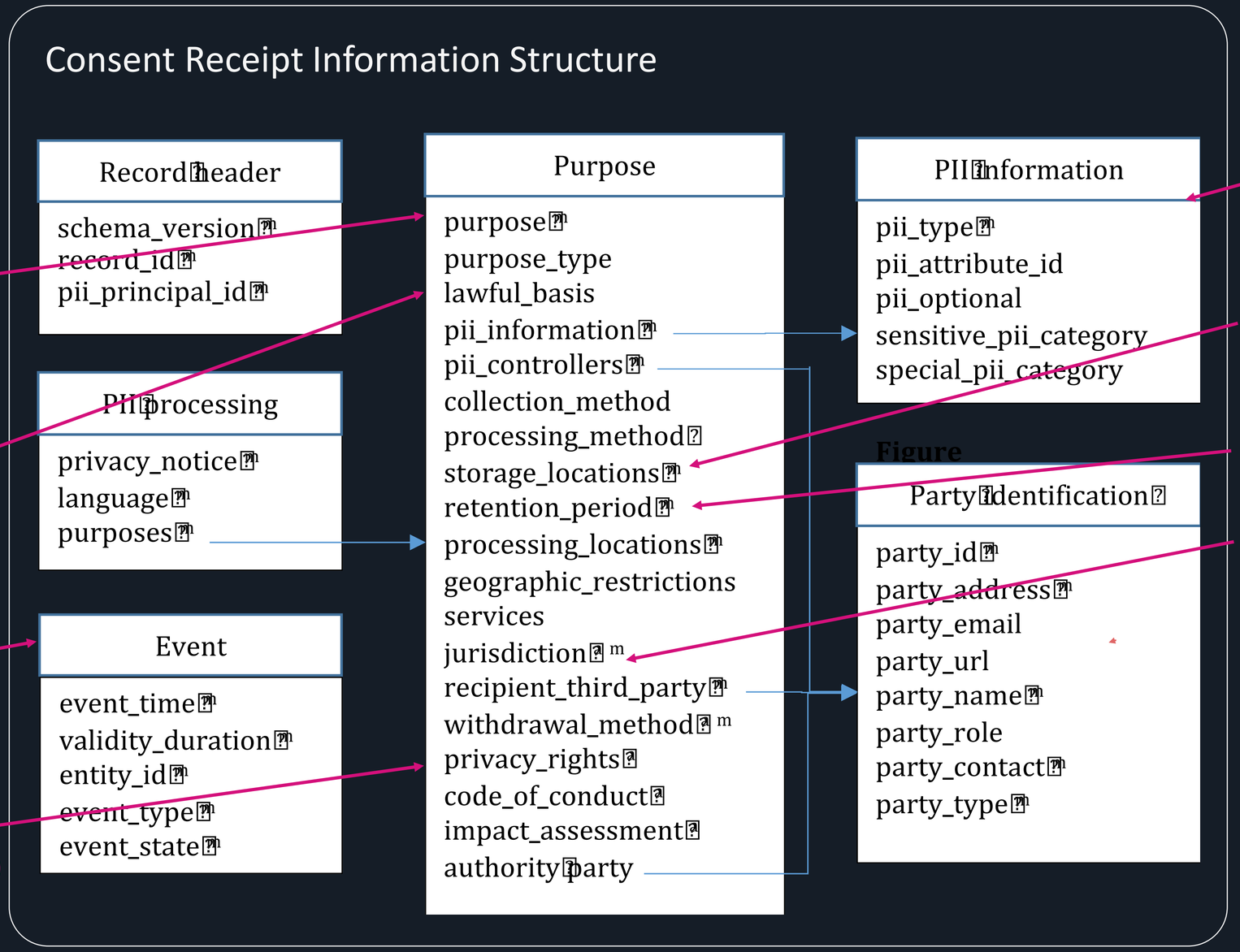
Open ID Connect



Apple App Store



ISO/IEC 27560 CONSENT RECORD AND RECEIPT STRUCTURE



CONSENT RECEIPT EXAMPLES (KANTARA)

CRYPTOMATHIC

Consent Receipt[1]

Version	KI-CR-v1.1.0
Jurisdiction	Discworld
Consent Timestamp	11/13/2017, 12:00:00 PM EST
Collection Method	Web Subscription Form with opt-in for marketing
Consent Receipt ID	c1befd3e-b7e5-4ea6-8688-e9a565aade21
Public Key	04:a3:1d:40:53:f0:4b:f1:f9:1b:b2:3a:83:a9:d1: 40:02:cc:31:b6:4a:77:bf:5e:a0:db:4f:ea:d2:07: c4:23:57:6f:83:2c:3d:3e:8d:e7:02:71:60:54:01: f4:6a:fb:a2:1e:8b:42:53:33:78:68:d9:7d:5e:b2: cc:0b:f8:a1:bf
Language	English

Consent Parties

Information Subject

PII Principle ID	**Bowden Jeffries**

Information Controller

PII Controller Name	**Ankh-Morpork Times**
PII Controller Contact	William de Word, Chief Editor & Data Protection Officer
PII Controller Address	Ankh-Morpork Times Gleam Street, Ankh-Morpork, Discworld
PII Controller Email	william@times.ankh-morpork.xyz
PII Controller Phone	(555) 555-DISC (3429)
PII Controller URL	https://www.times.ankh-morpork.xyz/contact
Privacy Policy	https://times.ankh-morpork.xzy/privacy_2017

Data, collection and use

Service	**Digital Subscription and News Alerts**

Purposes for collection and use

Purpose	*Purpose Category*	*Consent Type*	*PII Categories*	*Primary purpose?*
Fulfil Digital Subscription	Provision of services	EXPLICIT	• Technical • Demographics • Financial • Contact	TRUE
Marketing	Marketing	EXPLICIT	• Demographics • Financial • Contact	FALSE
Financial Record Keeping	Fiduciary obligation	N/A	• Financial	FALSE
Law Enforcement	Legal obligation	N/A	• All	FALSE

Termination	https://times.ankh-morpork.xzy/privacy_2017#termination
Third Party Disclosure	**True**
Third Party Names	• Outsourced printer • Outsourced fulfillment vendor • Bank • Law enforcement with subpoena • Digital Advertising Agency
Sensitive PII	**Yes**
Sensitive PII Category	**Financial Information**

kantara™ INITIATIVE

SECURITY EXPECTATIONS CONTRAST

Contrast on the expectations on execution environment

Managed Infrastructure

Hardware Security Module (HSM) security

- Key management
- Isolated with strict access control
- Hardware integrity (FIPS 140-2 level 3)

KEY MANAGEMENT

PAYMENTS

DIGITAL IDENTITIES & SIGNATURES

Unmanaged Devices

Mobile security

- Apple secure enclave
- Android key store
- StrongBox

MOBILE APP SECURITY

Examples of issues

- Qualcomm TEE (Trusted Execution Environment) vulnerability CVE-2019-10574
- Samsung TEE vulnerability SVE-2018-12853
- Huawei TEE vulnerability CVE-2017-8142
- Apple Secure enclave issue reported on MacWorld

SECURITY VULNERABILITY ASSESSMENT OVERVIEW

Overview of the regulation, execution environment and assessment

Regulation

NIST	eIDAS2	CyberSecurityAct
IAL3	High	High
IAL2	Substantial	Substantial
IAL3	Low	Basic

Environment

Managed

Unmanaged

Assessment

Common Criteria (ISO/IEC 15408)

Vulnerability Assessment	Security design and impl.
AVA_VAN.5	EAL7
AVA_VAN.4+	EAL6
AVA_VAN.4	EAL5
AVA_VAN.3	EAL4
AVA_VAN.2	EAL3
AVA_VAN.1	EAL2
	EAL1

SECURITY VULNERABILITY ASSESSMENT OVERVIEW (PAYMENTS)

Overview of the regulation, execution environment and assessment

Assessment

Payment Systems (PCI)

- PCI-DSS
- PCI-PTS
- PCI-MCOTS/ MPOC

Environment

Managed

Unmanaged

Assessment

Common Criteria (ISO/IEC 15408)

Vulnerability Assessment	Security design and impl.
AVA_VAN.5	EAL7
AVA_VAN.4+	EAL6
AVA_VAN.4	EAL5
AVA_VAN.3	EAL4
AVA_VAN.2	EAL3
AVA_VAN.1	EAL2
	EAL1

DESIGNING, OPERATING AND MAINTAINING AN APP WITH HIGHLY SENSITIVE DATA COMES WITH AN ENORMOUS LIABILITY

CRYPTOMATHiC

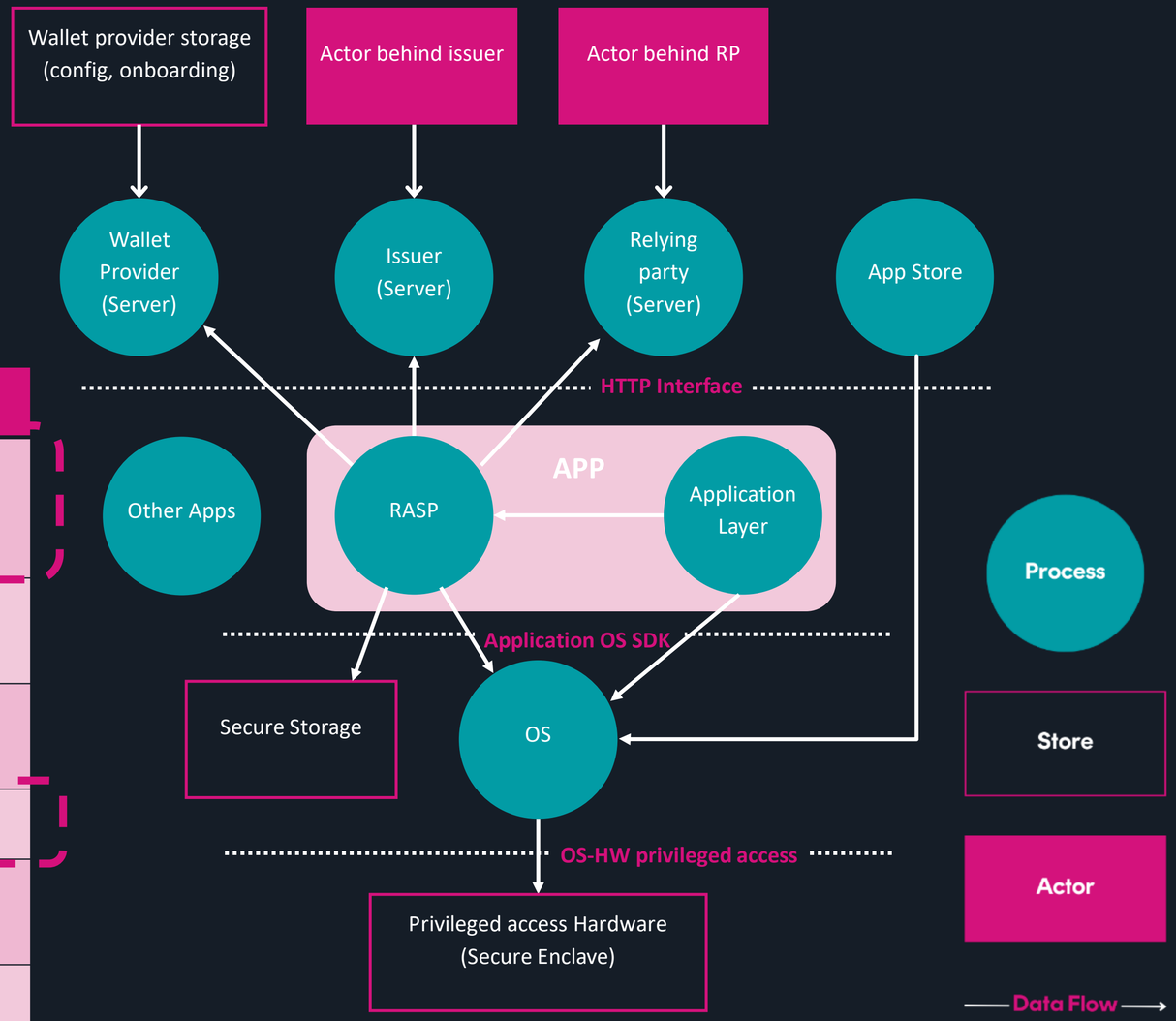
Examples of threat agents are numerous and include:

1. Lost/stolen mobile device in the hands of a threat actor
2. Malware installed on the device to log user credentials, output, or probe the app (malicious overlays and screen casting tools)
3. Jailbroken/rooted devices.
   A jailbroken device offers less OS guarantees and a rooted device
4. A compromised or monitored network that allows eavesdropping or altered network communications
5. Mobile apps that incorrectly implement security mechanisms of the underlying mobile app platform
6. Repackaged apps on the mobile device hosting the wallet that interact with the wallet
7. Poor code quality can lead to the discovery of vulnerabilities that the attacker can exploit
8. Disgruntled employees may share secret keys associated with app and open for illegal access

OWASP THREAT MODELLING TOOL

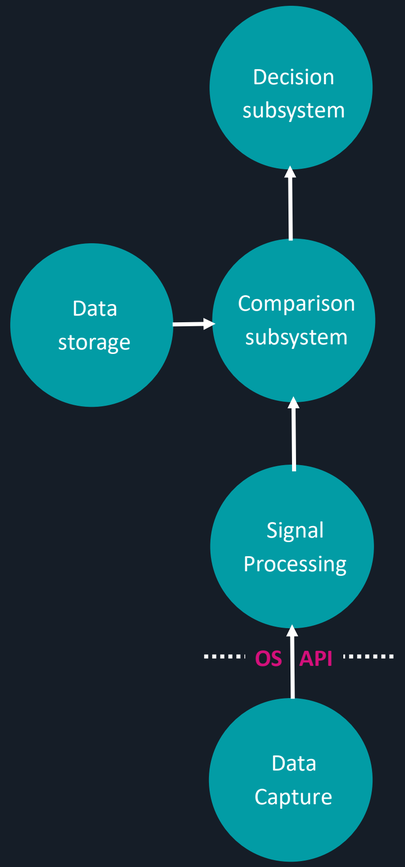
OWASP Threat Dragon is a modelling tool used to create threat model diagrams as part of a secure development lifecycle.

Category	Description	Required security measure
Spoofing	An unauthorized service masquerading as a participant in the EUDI wallet scheme interacts with a legitimate EUDI wallet to obtain personal data or authentication secrets from the wallet.	Authenticity
Tampering	Unauthorized modification of the EUDI wallet source code or runtime operations to alters its data flow and control environment.	Integrity
Repudiation	Vulnerabilities in access controls to the EUDI wallet or cryptographic key material prevents definitive proof that a person performed a specific action.	Non-repudiation
Information Disclosure	The EUDI wallet exposes sensitive information to individuals who are not authorized to have access to it.	Confidentiality
Denial of Service	Degrading or denying use of the EUDI wallet to the point where it adversely affects valid users from performing routine tasks.	Availability
Elevation of Privilege	Exploiting a vulnerability in EUDI wallet to gain access elevated access permissions within the wallet to extract secrets or sensitive information.	Authorization

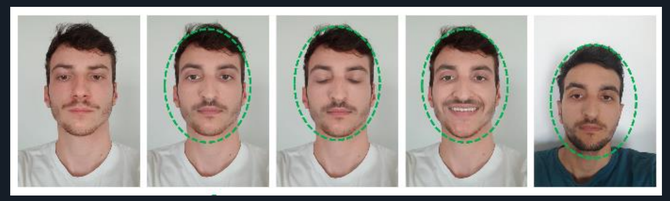


VIDEO CAPTURE VULNERABILITY ASSESSMENTS AND THREATS

OWASP Threat Dragon is a modelling tool used to create threat model diagrams as part of a secure development lifecycle.



How video injection attacks can even challenge state-of-the-art Face Presentation Attack Detection Systems (2023)



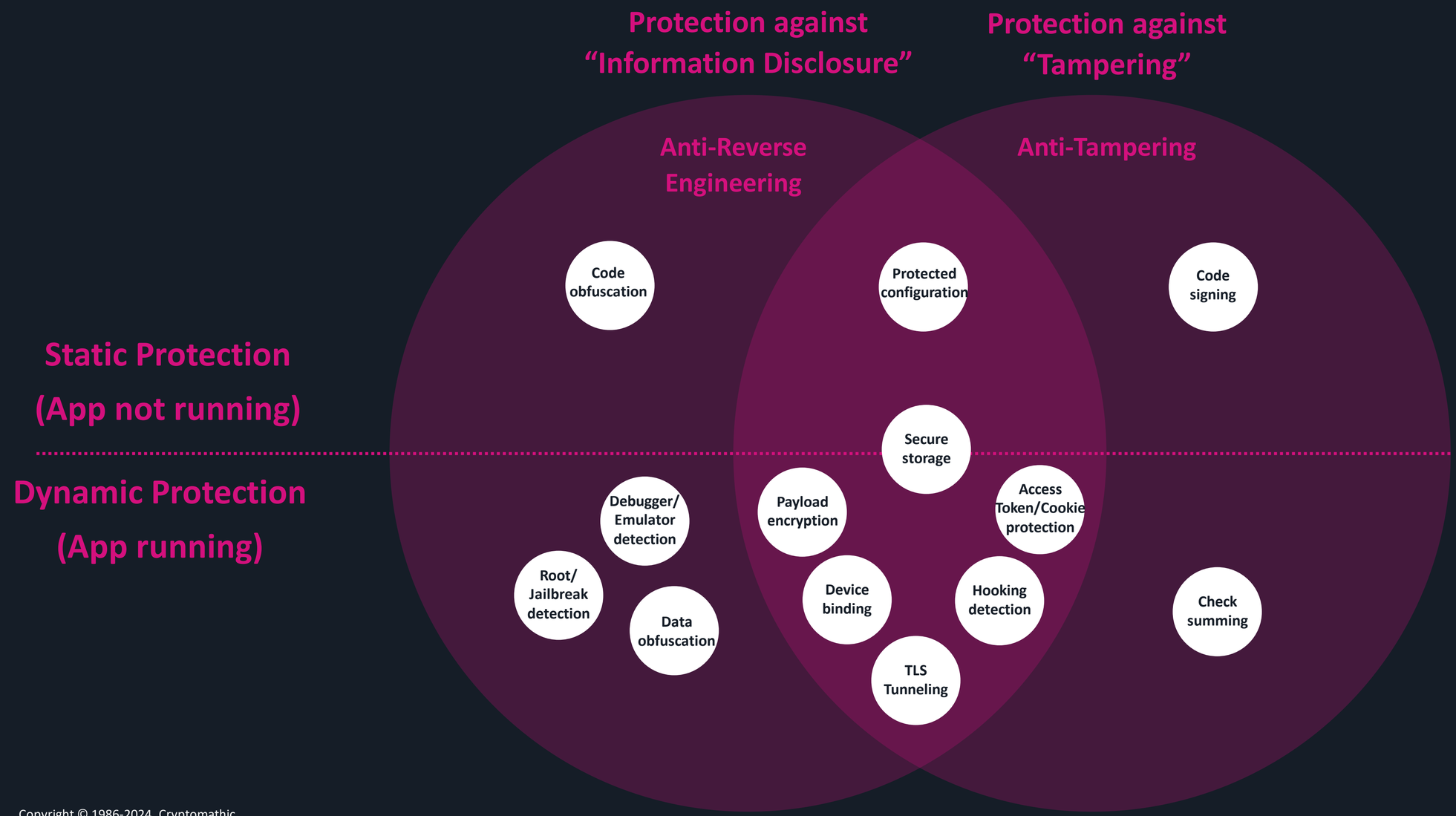
Process

Store

Actor

Data Flow

CONSIDERING THE THREAT MODEL WHEN DEVELOPING AN APP



SECURITY MEASURES AND TECHNIQUES

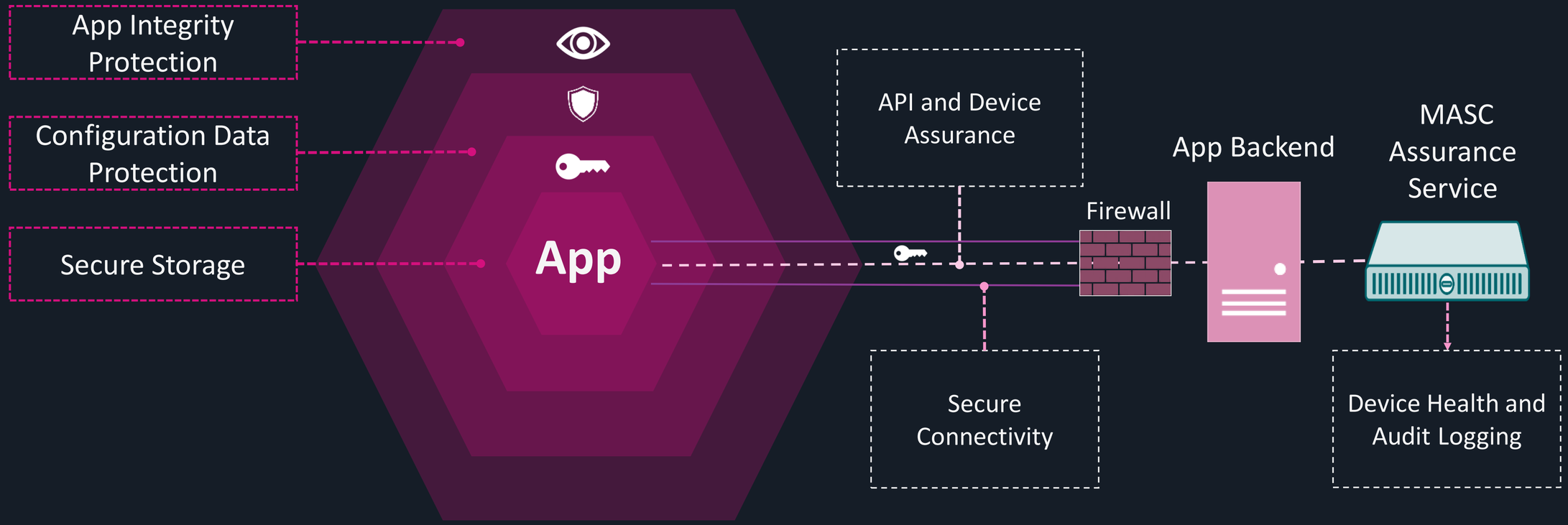
What kind of techniques can be used to address the security measures

Secure storage	(1) (2) (3)
Code obfuscation	(4)
Data obfuscation	(2)
Protected configuration	(1) (2)
Code signing	(5)
Detection/ prevention of: emulators/ debuggers rooted/ jailbroken devices	(6)
Detection/ prevention of: • hooking tools	(6)
Device binding	(1) (2) (7) (8)
TLS Tunnelling	(9) (10)
Payload Encryption	(1) (2)
Access Token / Cookie Protection	(1) (2)
Check summing	(11)

(1) Cryptography
(2) White-box cryptography
(3) Integration with platform authentication mechanisms
(4) Automated obfuscation tools
(5) Code signing using PKI certificates
(6) Host monitoring
(7) Device fingerprinting
(8) Secure enrolment with back-end servers
(9) Authorized server white list
(10) Certificate pinning
(11) Check sums

INTRODUCING MASC ARCHITECTURE

Mobile Application Security Core - Layered Security



Secure Storage
- Extending OS key stores
- Independent cryptographic functions
- Prevent data separation

Configuration Data Protection
- license keys
- API keys
- backend host names
- certificates

App Integrity Protection
- Anti-Dubug
- Anti-Tamper
- Root and Jailbreak Detection
- Emulator Detection
- Remote Desktop Detection

Secure Connectivity
- Separate root certificates
- HTTPS tunneling (whitelists)
- Extra encrypted layer
- OAuth2 token protection
- Cookie protection
- Token replacements
- Remote update

API and Device Assurance
- Challenge-response protocol establishes genuine app
- Device-unique binding
- Secure communication

Device Health
- Sentinel health message
- Audit logs
- Monitor device integrity and response

MASC COMPLIANCE WITH MOBILE SEC REQUIREMENTS

	ENISA Domain	# ENISA Security Measures	#ENISA Security Measures Relevant to Mobile App Security Solutions	# MASC Supported ENISA Security Measures
1	Handle runtime code interpretation correctly	6	1	1
2	Secure data integration with third party code	5	1	1
3	Protect the application from client-side injections	16	4	4
4	Handle authentication and authorization factors securely on the device	9	6	6
5	Identify and protect sensitive data on the mobile device	34	12	11
6	Ensure sensitive data is protected in transit	13	11	11
7	Check device and application integrity	5	4	3
8	Secure software distribution	8	0	0
9	Consent and privacy protection	15	2	1
10	Implement user authentication, authorization and session management correctly	19	4	4
11	Protect paid resources	6	0	0
12	Secure the backend services, the platform serves and APIs	7	0	0
13	Ensure correct usage of biometric sensors and secure hardware	9	2	2
	TOTAL	152	47	44 (94%)

	OWASP MAS Requirements Category	# MAS Requirements	# MAS Requirements Relevant to Mobile App Security Solutions	# Relevant MAS Requirements for which MASC Provides Support
1	Architecture, Design and Threat Modeling	12	2	1
2	Data Storage and Privacy	15	9	9
3	Cryptography	6	6	6
4	Authentication and Session Management	12	4	4
5	Network Communication	6	5	5
6	Platform Interaction	11	8	7
7	Code Quality and Build Setting	9	5	5
8	Resilience	13	13	12
	TOTAL	84	52	49 (94%)

OVERVIEW

Goal 1: Role of the mobile towards secure cloud service (use cases)

Goal 2: Transparency with processing notice

Goal 3: Overview NIST and EU Security Regulation and Assessment

Goal 4: Understanding security threats and mitigation

THANK YOU

CRYPTOMATHiC

+46 (0) 730684942

Jan.lindquist@cryptomathic.com

JAN LINDQUIST
Product Manager
Mobile Application
Security Core