New Queensland Driver Licence (NQDL)

A real ISO/IEC 24727 implementation

Queensland

Presentation overview

- What are the NQDL objectives?
- What were the choices?
- NQDL goals
- What is on the licence?
- Stakeholder values
- Implementation platform
- Implementation decision i.e. ISO/IEC 24727
- Implementation issues
- Department of Transport and Main Roads developed ISO/IEC 24727 authentication protocols
- Final product

Queensland Government

What are the business objectives?

- Improve the integrity and security of the driver licence.
- Improve convenience and services for Queensland licence holders while providing a platform for electronic service delivery.
- Deliver a better return on Government’s investment.

What were the choices?

Security →

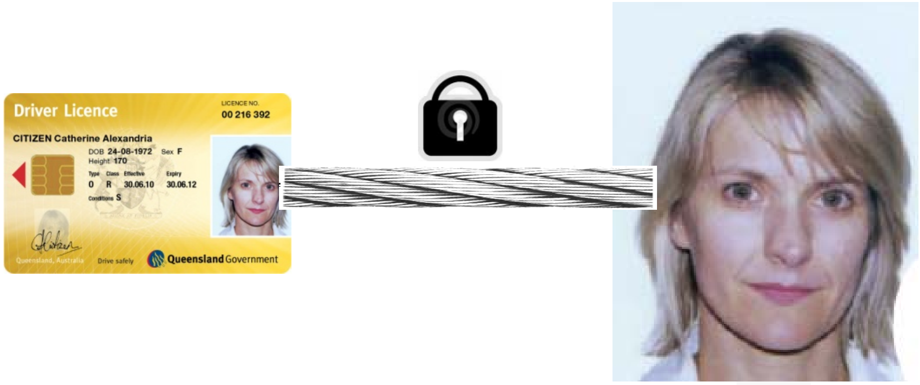
Feature	Option 1	Option 2	Option 3
Introduce digital cameras	✓	✓	✓
Store facial and signature images		✓	✓
Production location	Local	Central	Central
Finished product	Plastic Card 	Plastic Card 	Smartcard

Note: Smartcard design indicative only

Queensland Government

NQDL goals

One driver = one licence



Business

A multi-strand approach:

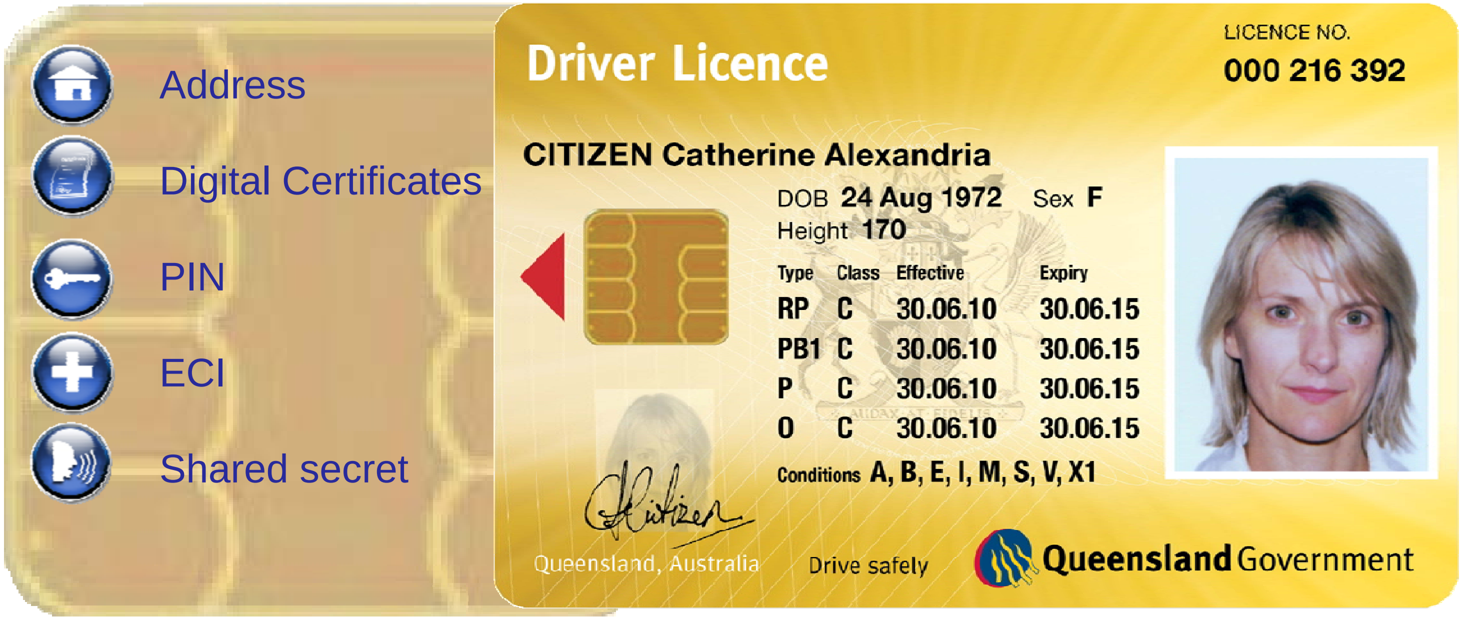
- Enrolment procedures (business process)
- Physical document security (forgery & tampering)
- Electronic verification of breeder documents
- Biometric verification and identification
- Electronic document security

Technology

Note: Smartcard design indicative only

Queensland Government

What is on the licence?



- Address
- Digital Certificates
- PIN
- ECI
- Shared secret

Driver Licence

LICENCE NO.
000 216 392

CITIZEN Catherine Alexandria

DOB **24 Aug 1972** Sex **F**
Height **170**

Type	Class	Effective	Expiry
RP	C	30.06.10	30.06.15
PB1	C	30.06.10	30.06.15
P	C	30.06.10	30.06.15
O	C	30.06.10	30.06.15

Conditions **A, B, E, I, M, S, V, X1**

C Citizen

Queensland, Australia

Drive safely

Queensland Government

Government **Card Holder** **Third Parties**

Note: Smartcard design indicative only

Stakeholder values

Government

- Enables eBusiness
- Reduces ID fraud.
- Delivers interoperability between government smartcard implementations
- Lowers development cost for government through re-use

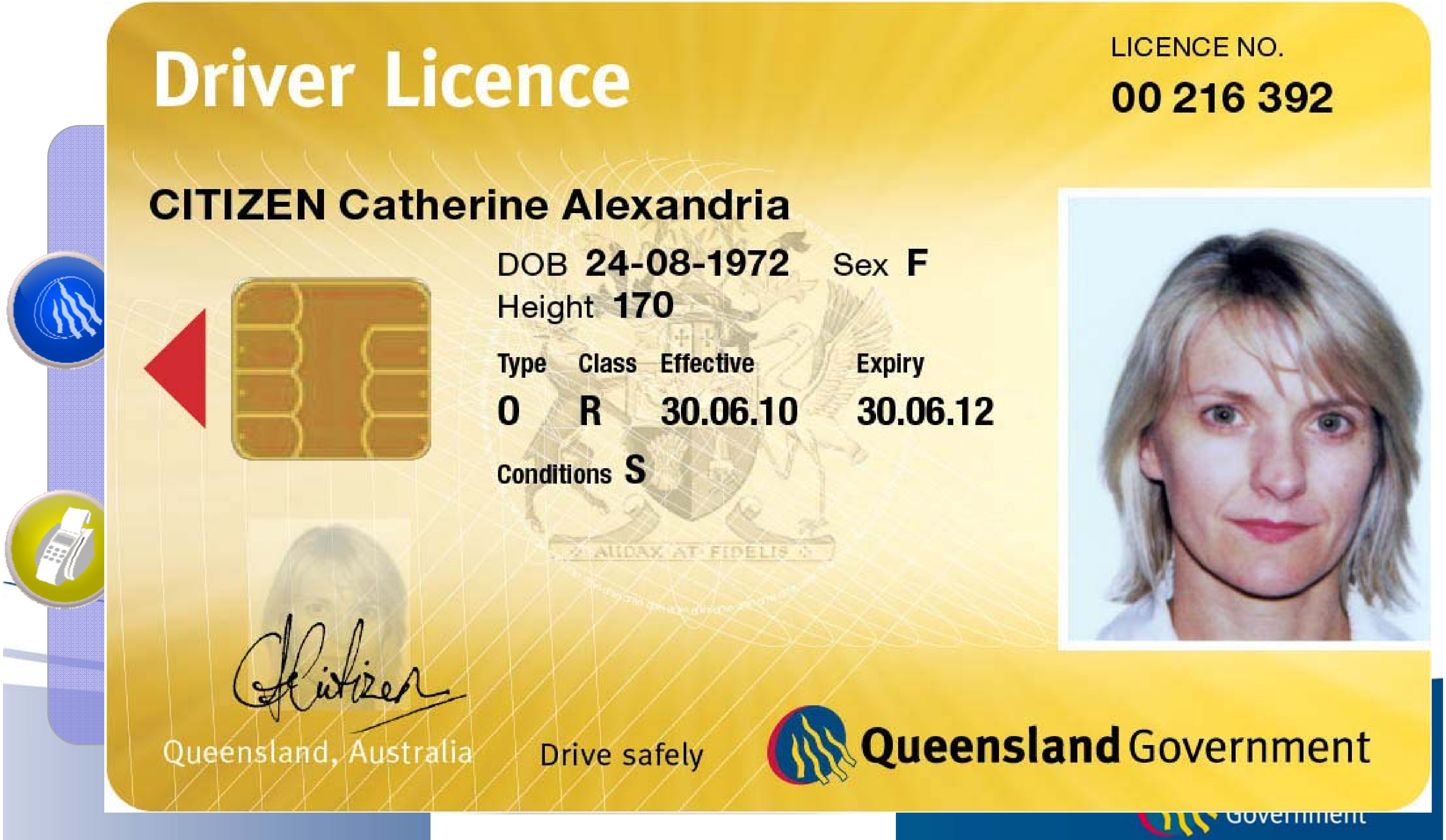
Card holder

- Increased control over personal information
- Reduces risk of identity theft.
- Enhanced authentication to DTMR business over the web.

Third parties

- Increased confidence in the authenticity of smartcard products.
- Leverage the smartcard as an authentication mechanism
- Enable third party applications to interact, ie, Age Attainment

Implementation platform



Driver Licence

LICENCE NO.
00 216 392

CITIZEN Catherine Alexandria

DOB 24-08-1972 Sex F
Height 170

Type	Class	Effective	Expiry
O	R	30.06.10	30.06.12

Conditions S

Queensland, Australia

Drive safely

Queensland Government

Note: Smartcard design indicative only

Implementation decision

- ISO/IEC 24727 ICC-Resident stack model
- 144 kilo byte JavaCard 2.2.1

Why the ICC-Resident stack model?

- Green field implementation.
- SAL API is the only smartcard API that is defined in ASN.1 and is totally un-ambiguous.
- Does not require procedural elements.
- Does not require Cryptographic Information Application (CIA).
- Future proof for non APDU based cards, e.g. TLS Internet cards or JavaCard 3 cards.
- Does not require off-card translation between on-card and off-card concepts, which simplifies discoverability.

Implementation issues

- Due to the ASN.1 DER encoding the payload to and from the smartcard is larger
- Needed to write a DER encoder/decoder for the on-card implementation, but JavaCard 2.2.2 should provide at least BER encoding functionality.
- Loading of initial DID. How is the initial DID loaded securely? (Detailed in later slide)
- Size of on-card code due to DER encoder/decoder
- Secure post issuance. (Detailed in later slide)
- Implementing the ICC-Resident stack through HTTPS. (Detailed in later slide)

Implementation issues – Loading of initial DIDs

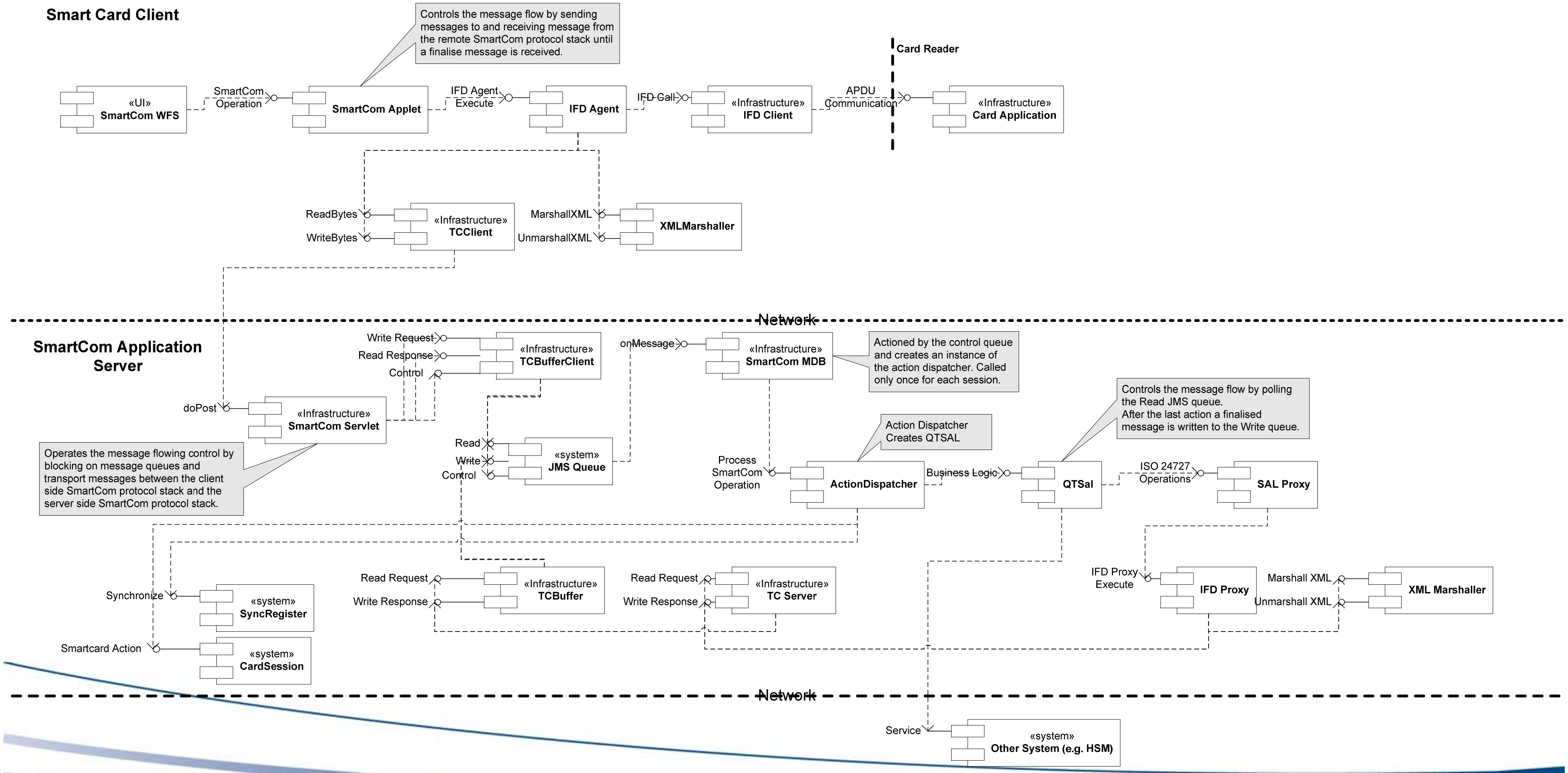
- How are the initial DIDs loaded securely
  - TMR follows best security practice by ensuring that all key transport is done in a secure manner and never in clear text. This is achieved by:
    - Using Global Platform SCP02 secure messaging for the initial DIDs
    - Using the TMR developed key transport mechanism in authentication protocol creation and updates
  - Once the initial DIDs are loaded GP is not used for any further key transport. ISO/IEC 24727 mechanism are used from thereon.

Implementation issues – Secure post issuance

- TMR requires a secure mechanism to install new or update existing smartcard functionality in a secure way.
- Post issuance must be possible over a remote network.
- Because security objects (such as secret/private keys, PINs etc…) must never leave the smartcard it was necessary to separate the functionality from the data stored on the card. This enables the code base to be deleted and re-installed without affecting the data stored on the smartcard.
- The GlobalPlatform card manager and SCP02 is used to install the CAP files.
- The secure session is established from the smartcard issuer to the smartcard.

Queensland Government

Implementation issues – ICC-Resident stack through HTTPS



Controls the message flow by sending messages to and receiving message from the remote SmartCom protocol stack until a finalise message is received.

Actioned by the control queue and creates an instance of the action dispatcher. Called only once for each session.

Controls the message flow by polling the Read JMS queue.
After the last action a finalised message is written to the Write queue.

Action Dispatcher Creates QTSAL

Operates the message flowing control by blocking on message queues and transport messages between the client side SmartCom protocol stack and the server side SmartCom protocol stack.

Department of Transport and Main Roads developed ISO/IEC 24727 authentication protocols

- Transport Key Specification Protocol
- Client Application Symmetric Session Key Establishment Protocol
- Client Application Symmetric Mutual Authenticate with Session Key Establishment Protocol
- Client-Application Secure PIN Compare Authentication Protocol
- Client Application Shared Secret Authentication Protocol

Department of Transport and Main Roads developed ISO/IEC 24727 authentication protocols (continued)

- Client Application Asymmetric Internal Authentication Protocol
- Client Application External Authenticate with Certificates Protocol
- Age Attainment Authentication Protocol
- ICC State Authorisation Protocol

Transport Key Specification Protocol

- The smartcard asymmetric key pair is used to secure key transport between the off-card application and the smartcard application.
- Supported transport mechanisms:
  - EnvelopedSecretData – Cut down version of PKCS#7
  - rsaPKCS#1
  - rsaPKCS#1 – OAEP
  - rawRSA
  - GlobalPlatform SCP02

Client Application Symmetric Session Key Establishment Protocol

- A session key establishment protocol allowing a symmetric session key to be established by the ISO/IEC 24727-3 implementation.
- The smartcard asymmetric key pair may be used to provide smartcard credential authentication.

Client Application Symmetric Mutual Authenticate with Session Key Establishment Protocol

- A symmetric mutual authenticate with session key establishment protocol allowing symmetric session keys to be established by the ISO/IEC 24727-3 implementation.

Client-Application Secure PIN Compare Authentication Protocol

- A PIN-based authentication protocol in which the PIN is transmitted to a card-application in encrypted form.
- Uses EMV PIN block format

Client Application Shared Secret Authentication Protocol

- An authentication protocol allowing a card holder to authenticate to the smartcard using a predefined set of questions and answers, referred to as shared secret.
- The following are the objectives of this protocol:
  - The protocol is designed to offer the cardholder a mechanism to authenticate in a secure way using secrets that can be easily remembered.
  - Provide a mechanism to create the differential identity for this authentication protocol that allows for the shared secret answer to be transported to the smartcard in a secure fashion during the DIDCreate and DIDUpdate.

Client Application Asymmetric Internal Authentication Protocol

- The smartcard asymmetric key pair may be used to provide smartcard credential authentication.
- This authentication protocol is a challenge/response protocol using public key cryptography.

Client Application External Authenticate with Certificates Protocol

- A client application asymmetric external authentication with certificates protocol that caters for on-card certificate verification, with an optional access profile defined as a didNameList.
- Developed to manage third party access to smartcard data without the need to create new security conditions within the ACLs of the requested targets.
- The didNameList is contained within custom X.509 certificate extensions.
- Cross certification may be required between interested parties PKI hierarchies.
- This protocol uses internal DIDs containing the simple assertion authentication protocol.
- The security condition for the DIDAuthenticate function on the DIDs containing the simple assertion authentication protocol must be set to never.

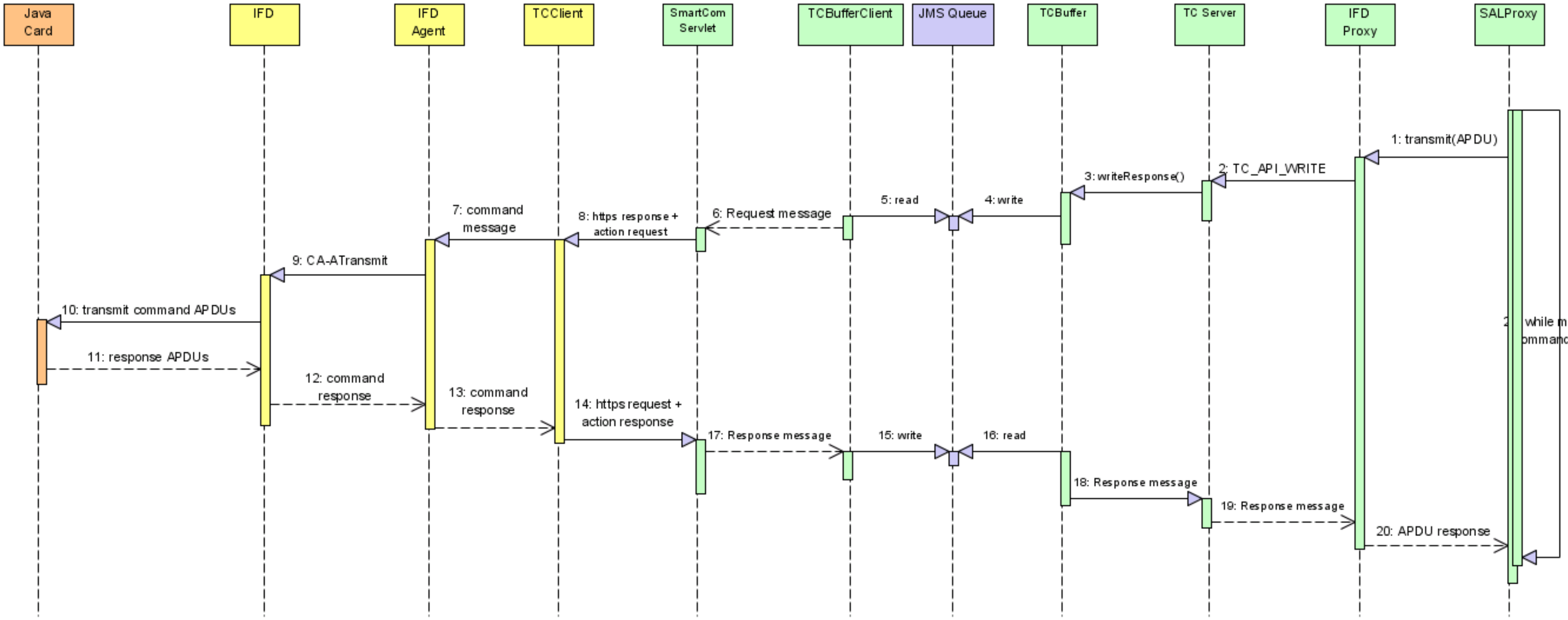
Age Attainment Authentication Protocol

- An authentication protocol that allows a card holder to prove that he/she has attained a specific age, without releasing the cardholder's date of birth.

ICC State Authorisation Protocol

- This protocol was designed to manage the life cycle of the ICC.
- Global Platform ICC management could not be used because it was a requirement to lock and possible un-lock the card in the future.
- The ICC state authorisation protocol allowing certain actions associated with targets based on the state of the ICC.
- This authorisation protocol defines the current state of the ICC and its containing applications.
- The authentication state is implicitly set to “authenticated” only if the iccState is set to ‘1’ i.e. ACTIVE.
- The authorisation protocol state is set when a connection to the ICC is established.

Final product – Sequence Diagram



Final product

- The first ISO/IEC 24727 implementation in Australia
- Use of the ICC-Resident stack model
- JavaCard 2.2.1 technology
- Remote smartcard interaction
- Secure DIDCreation
- Flexible authentication protocols

Demonstration

Reference Implementation available soon:

https://www.govdex.gov.au/confluence/display/SIRIUS/

Queensland Government

Questions?

Thank you

Alexander Gagel
Principal Advisor (Solutions Architecture)
New Queensland Driver Licence
Enterprise Information and Systems Division
Department of Transport and Main Roads
Email: alexander.z.gagel@tmr.qld.gov.au

New Queensland Driver Licence
Email: newlicence@tmr.qld.gov.au
Mail: New Queensland Driver Licence Project
GPO Box 1412 Brisbane Qld 4001