ISO/IEC 24727 Tutorial
Access Controls Pre & Post ISO/IEC 24727

NIST

Why do we use Access Controls?

- Control access to on-card data
- Set the conditions under which an ICC will respond
- Use the ICC to enforce different business rules for different use-cases
- For government, this is often privacy related – we use the ICC to protect the card holder

Plain English Examples

- Certificate is always readable
- Retry counter is never readable
- DOB is readable if cardholder is authenticated and police is authenticated
- Log is readable if police is authenticated or customs is authenticated
- Certificate is not writable unless date is authenticated and certificate has not expired or Issuer is authenticated

NIST

Before 24727 – under ISO 7816-9

- Access control model was “flat” - did not allow for complex or nested conditions
- The range of authentication protocols was limited
- Implementations were often proprietary – ISO 7816-9 only defines the interface – not the implementation
- Application level coding (i.e. application logic) was required
- Most implementers were either forced to simplify their business requirements or were forced to develop their own “application”
- It was not possible to “standardize” the on-card application without extensive effort (e.g. EMV, GP, SIM)
- Application maintenance was an expensive long term cost

NIST

24727-3 Authorization Service

- The Authorization service creates & maintains Access Control Lists (ACLs)
- ACLs may contain Access Rules (ARs)
  - If set - the AR is enforced against requests addressing the target
  - If not set – then the DID can not be authenticated (i.e. equivalent to “NEVER”)
- The target of an ACL may be a:
  - card-application
  - data set
  - differential-identity
- ARs apply whenever an action against a target is performed

NIST

24727-3 Named Data Service

- Data sets and Data Structures for Interoperability (DSI) are created & maintained by the Named Data Service
- Data sets are maintained for each card application
  - Data sets are one of the Targets for ACLs
- DSI are maintained for each data set
  - There is no limit in the number of DSI per data set
  - DSIs contain the actual data in no specific format
  - DSIs are not targets and therefore not controlled by an ACL but rather by the ACL of the data set that they are contained in

NIST

24727-3 Differential Identity Service

- The differential identity service creates & maintains differential identities (DIDs)
- DIDs capture a DID Name, one Authentication Protocol (OID), a marker (or key) , a scope, and a qualifier
- DIDs have a (Boolean) state, either authenticated or not
- DIDs in the alpha card-application are implicitly global in scope
- DIDs in a card-application other than the alpha card-application are implicitly local in scope
- DIDs themselves are one of the targets for ACLs

NIST

Putting it together

- Data sets contain DSI which hold data
- Access Rules (ARs) are enforced against actions on a target (Application, Data Set, DID)
- ACLs contain ARs that are made up of security conditions, which need to be satisfied to allow a specific action to occur (i.e. setting the DID security state to true)

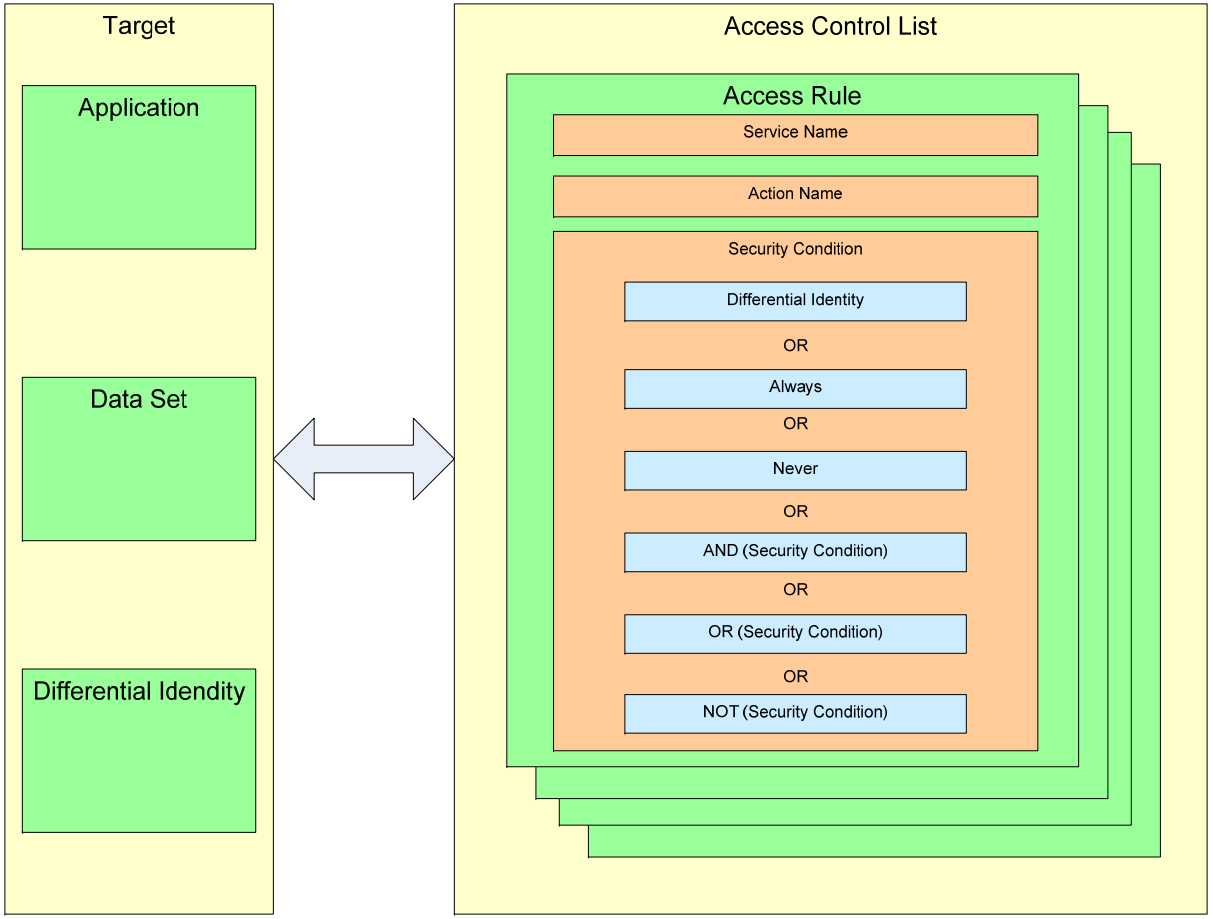
NIST

Putting it together (cont.)

- One or more Differential IDentities (DID) may be linked to each Target so that different authentication protocols or security conditions may be used for different access control requirements for the same target

NIST

ISO/IEC 24727 access control



NIST

AR example

NIST

Conclusion

- Access control model is hierarchical and supports multiple potential business rules at different levels
- The range of authentication protocols is expanded and extensible
- Implementations are no longer limited by ISO/IEC 7816
- No (Zero) Application level coding (i.e. application logic) is required even for complex business rules
- Business requirements no longer need to be restricted
- Application standardization is now very simple
- Application maintenance is much simpler and less costly

NIST

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

NIST