Managing the Contactless Interface

Mike Neumann
Director, Business Development, Americas
StepNexus, Inc.
Austin, TX USA

19-April-2006
Smart Card Alliance, Smart Cards in Government

STEPNEXUS™

Introduction

• Contactless smart card technology has been utilized for over a decade to facilitate convenient fare collection, payment and physical access

• To date, devices are typically issued for a single application purpose and supporting only a single interface

• Some transit applications, and now PIV, highlight a dual-interface architecture

• Access Control Rules now involve indicate interface restrictions for transmission of some data; privacy and security concerns are cited.

STEPNEXUS™

Application Management and Policy Projection

- Hard-Coded; implement access control to services in application code based on written policy (eg. PIV)

- Application Management Parameters – communicated today through proprietary extensions to LOAD commands

- Opportunity to utilize existing open specifications (ie. MULTOS secure package) via international standards (ISO 24727-3) to deploy and manage applications and content

- Compliant applications, terminals, handsets, services could exchange secure agreements on service and communications channel options

STEPNEXUS™

PIV

• Explicitly restricts data communicated via the contactless interface to only
  + CHUID
  + Card Authentication Certificate
  + PIV Application Version

• Explicitly restricts commands accessible via the contactless interface to only
  + SELECT
  + GET DATA
  + GENERAL AUTHENTICATE (if non-PIN ACR)

• Efficient implementation requires on-card API service to inform application of active communications interface.

Communication Interface Awareness

On-card APIs provide necessary tools to provide interface information to the on-card application.

MULTOS v4.2; void QueryInterfaceType(*int);

Java Card v2.2;
```
Class APDU {        ...
        public static byte APDU.getProtocol();
                ... };
```

STEPNEXUS™

Beyond PIV

• Interface Devices (IFDs) – Handsets, PDAs, SmartPhones; offer a variety of communications interfaces for service delivery

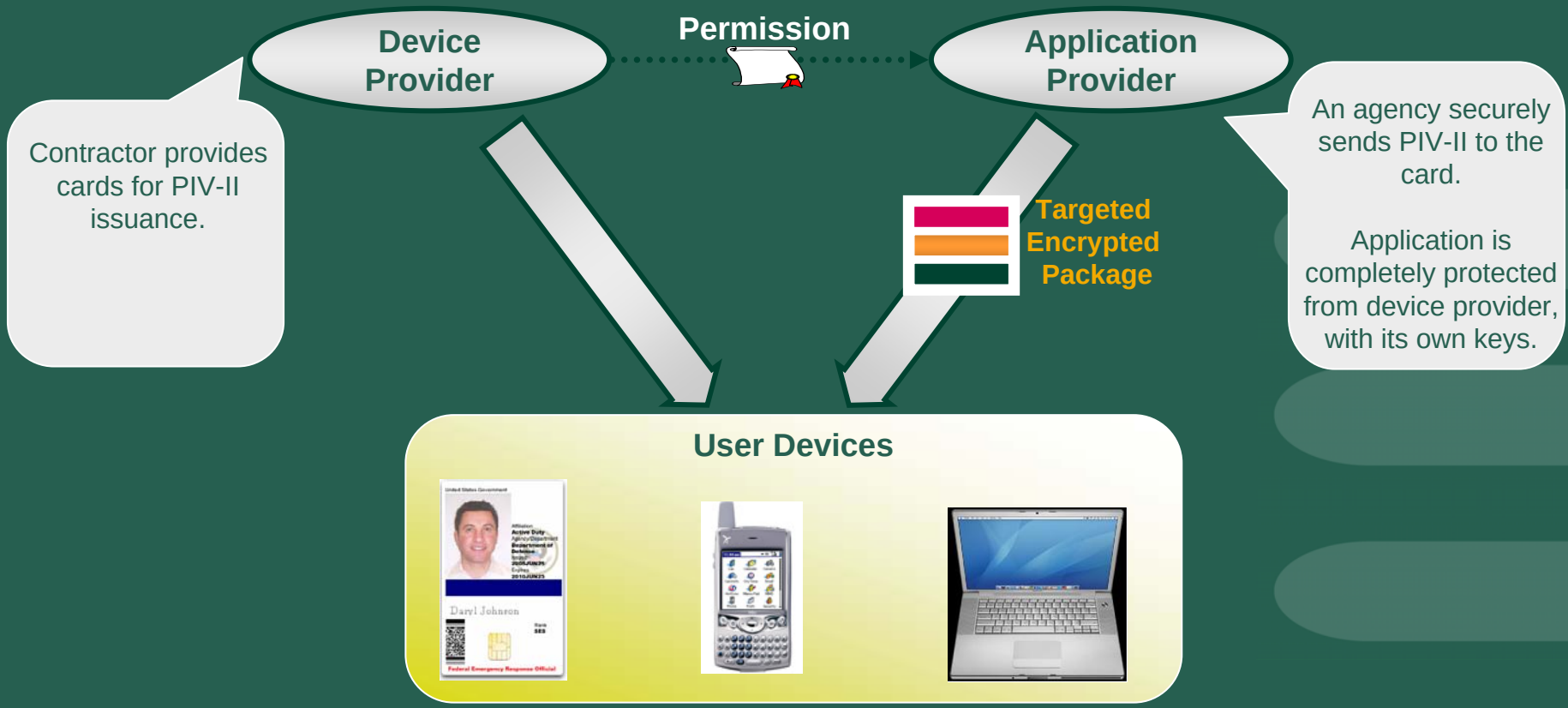
USB, WiFi, Bluetooth, GSM, CDMA, NFC, Certified Wireless USB

• On-card applications are increasingly responsible for enforcing their mode of use; including interface restrictions

• Applications may adaptively discover more efficient communications paths; eg. ‘boot’ with NFC to associate to a Bluetooth local network or WiFi hotspot.

• Interface utility decisions could be self-managed by the application or projected to the IFD

Independent Device and Application Control



- Only card capable of completely separating application privacy from the device, enabling different secure issuance models
- Perfect for separating agency applications from contractor applications
- Extremely important in offline situations, such as in emergencies, combat, or poor networks

STEPNEXUS™

Conclusions

• Capabilities for contactless communication are growing at an unprecedented rate

• Today's APIs support the required mechanisms for hard-coded application policy enforcement.

• Interface policy directives may be enforced via configurable applications.

•The StepNexus Application Management Scheme (MULTOS) uniquely offers an open, proven, mechanism for targeted device activation and application deployment and personalization.

Thank you

Mike Neumann
Director, Business Development, Americas
StepNexus, Inc.
9600 Great Hills Trail, Suite 150W
Austin, TX 78759 USA
+1 512 535 3080
mike.neumann@stepnexus.com