Identity and Client Security for Remote Access
- Virtual Credential Container -

Yukio Tsuruoka

NTT Information Sharing Platform Laboratories

Contents

- About NTT…
- Background
- Outline
- Client security
- Use case: remote access
- Solution: proof-of-concept demonstration
- Related topics
- Summary

Nippon Telegraph and Telephone (NTT) Corporation

NTT is a holding company conducting planning and R&D of telecommunication services

www.ntt.co.jp/index_e.html
(TSE:9432, NYSE: NTT)

Subsidiaries include:

- NTT East & NTT West - local operation in Japan
- NTT Communications - long distance and international telecommunication, IP networks, and ICT solutions

- NTT Data - system integration and network service

- NTT DoCoMo - mobile network operator

Reference: www.ntt.co.jp/about_e/corporatedata.html

NTT's services

- FTTH (provided by NTT East and NTT West)
  - 6 million subscribers, 177% growth rate
  - NGN commercial service has started
  - Planned: 20 million NGN subscribers by 2010

- Mobile network services (by NTT DoCoMo)
  - 53 million subscribers, 80% are 3G users
  - 7.2Mbps HSDPA access service has started

NTT's activities regarding identity management

- NTT Communications
  - Provides Single Sign-On (SSO) service to ISP (OCN) users
  - Users can access both OCN (7.7 million IDs) and "goo" sites (8 million IDs) using SSO via SAML 2.0

http://www.ntt.com/release/2007NEWS/0007/0702.html

- NTT Data
  - SSO achieved by ID Federation of intranet (20,000 IDs, 200 systems) and group company network (32,000 IDs, 20 systems)
- NTT Software
  - Identity federation module supports SAML 2.0:
  - TrustBind/Federation Manager

Background

- Enterprise concerns: risk of information leakage and legal compliance
- To increase manageability, enterprises tend to aggregate business information at one point
- Information is accessed from various locations (branch offices or outside the office) through a broadband access network
- Secure remote access is the key element to protecting corporate assets

Security of Remote Access

- Requirement: maintain secrecy of credentials
- Software-based credential container
  - Example: Windows certificate store
  - Credentials must be protected from malware
- Hardware-based credential container

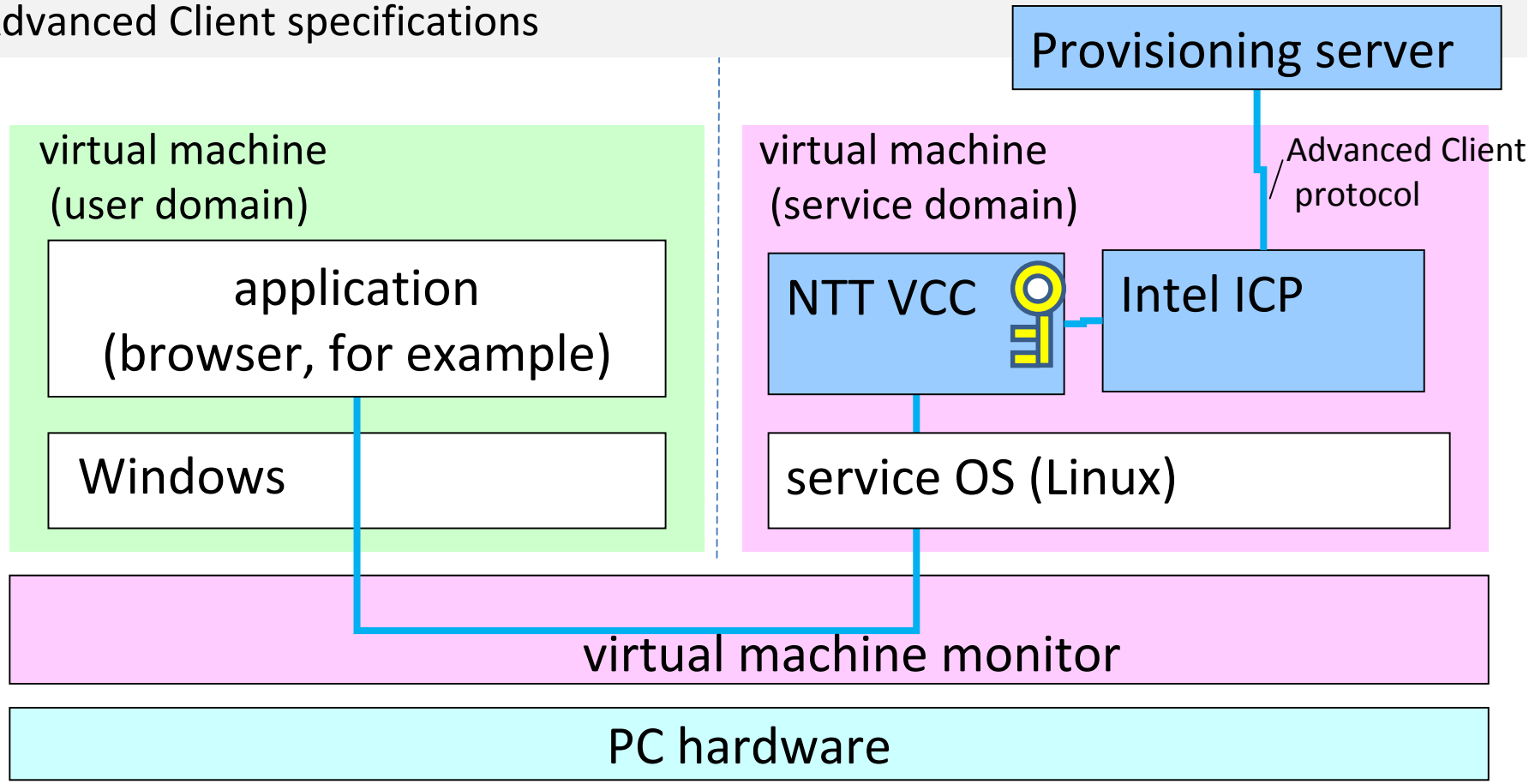
  (cryptographic token)
  - Example: USB cryptographic key
  - High security, but requires additional hardware cost and may be lost

Outline

- Problem
  - Protect credentials from malware in Windows
  - Minimize additional costs of protection
- Solution
  - Use virtualization for protection (Virtual Credential Container) and
  - Use standard protocols (Liberty Advanced Client) for provisioning of credentials
- Merit
  - Security of remote access strengthened with little additional cost (no external device needed)

Outline of solution – client configuration

NTT virtual credential container (VCC) stores credentials securely
Intel Identity capable platforms (ICP) provisions credentials based on Liberty Advanced Client specifications

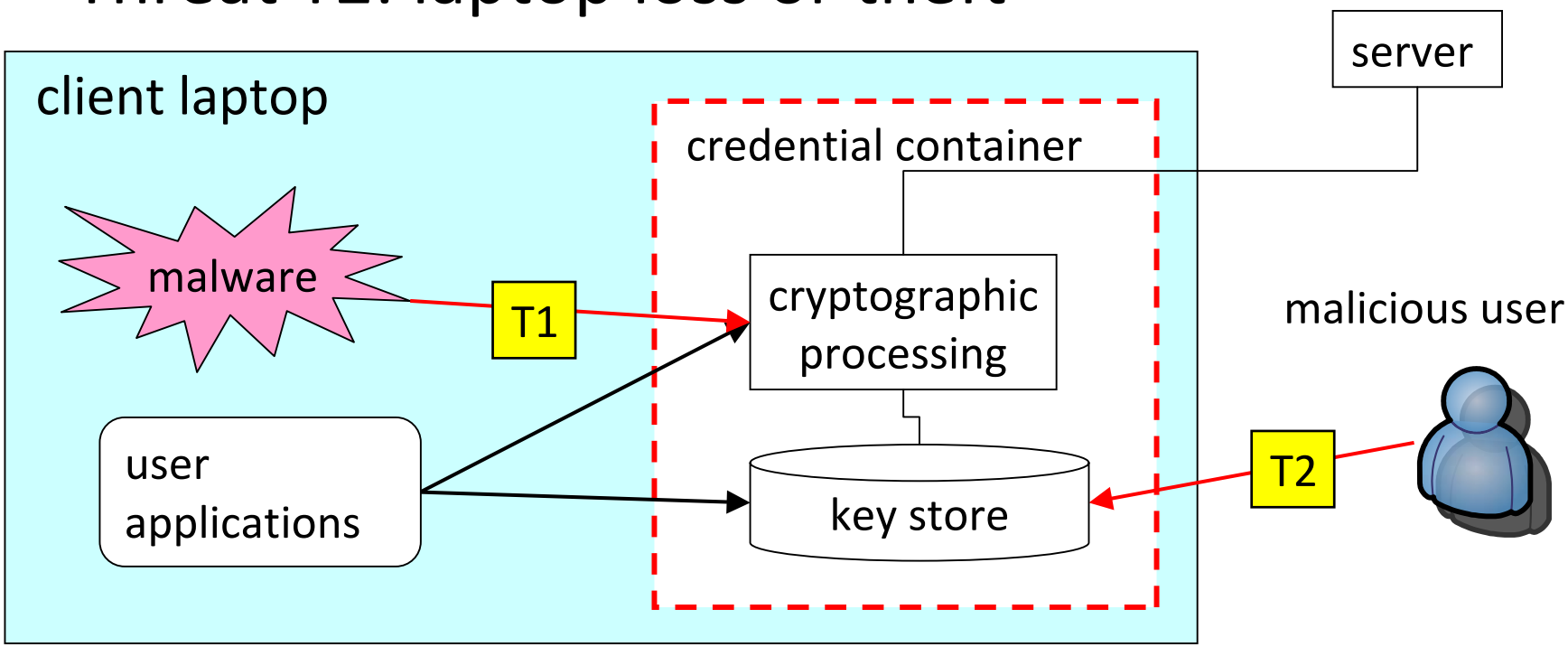


Client security can be strengthen without (the need for) external devices

Client security

Threats in user authentication

- Threat T1: malware attack
- Threat T2: laptop loss or theft

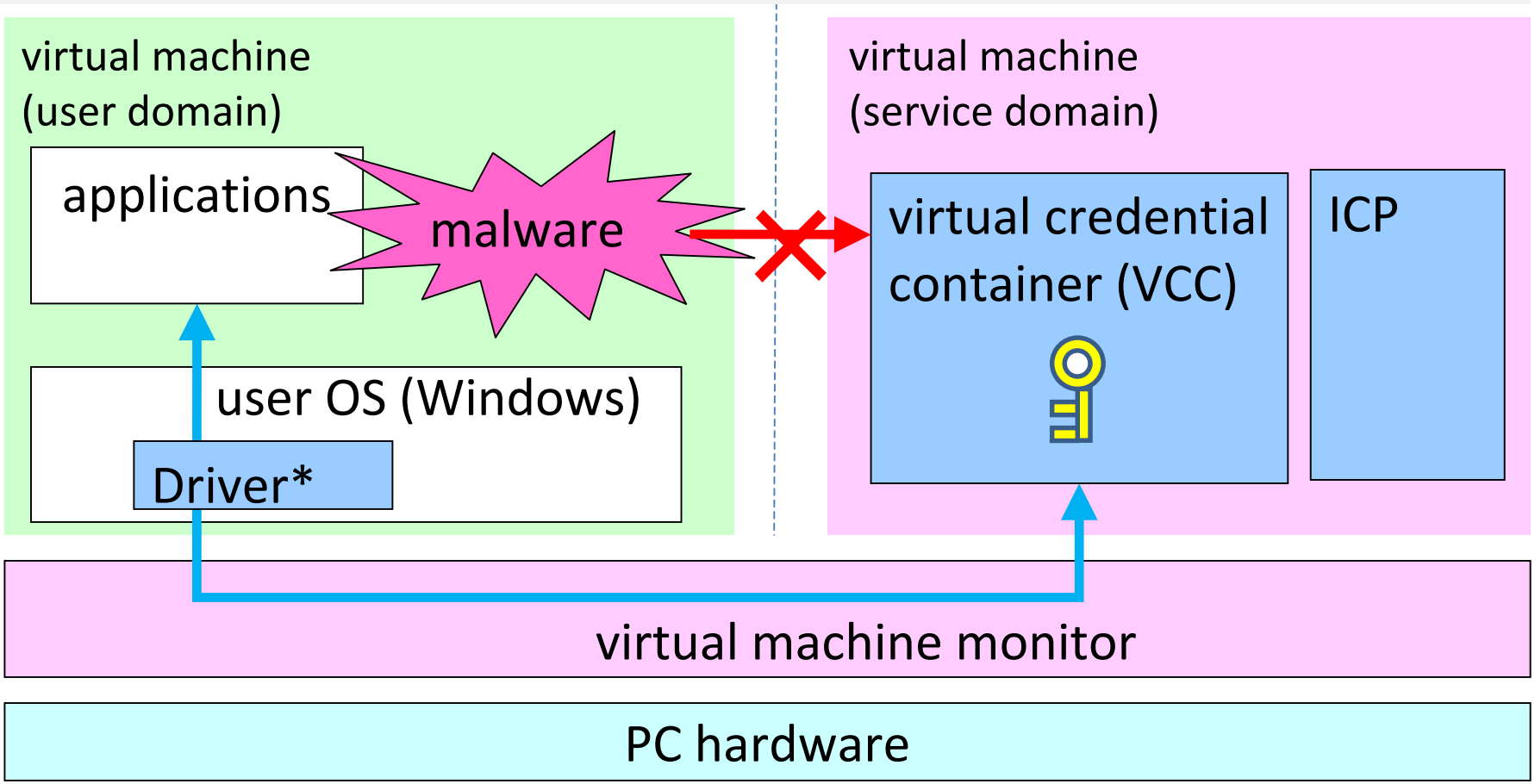


Countermeasures to malware (T1)

- Monitoring (Based on a black list)
  - Example: Virus scan by software
- Integrity check (based on a white list)
  - Check that the fundamental set of software is not forged.
  - Example: BIOS, OS, and drivers are checked.
- Minimizing the possible damage
  - Preventing key leakage even if application environment is infected by malware
  - Domain separation: split execution environments for critical operations (e.g., cryptographic operations) from that for applications

Domain separation by virtualization

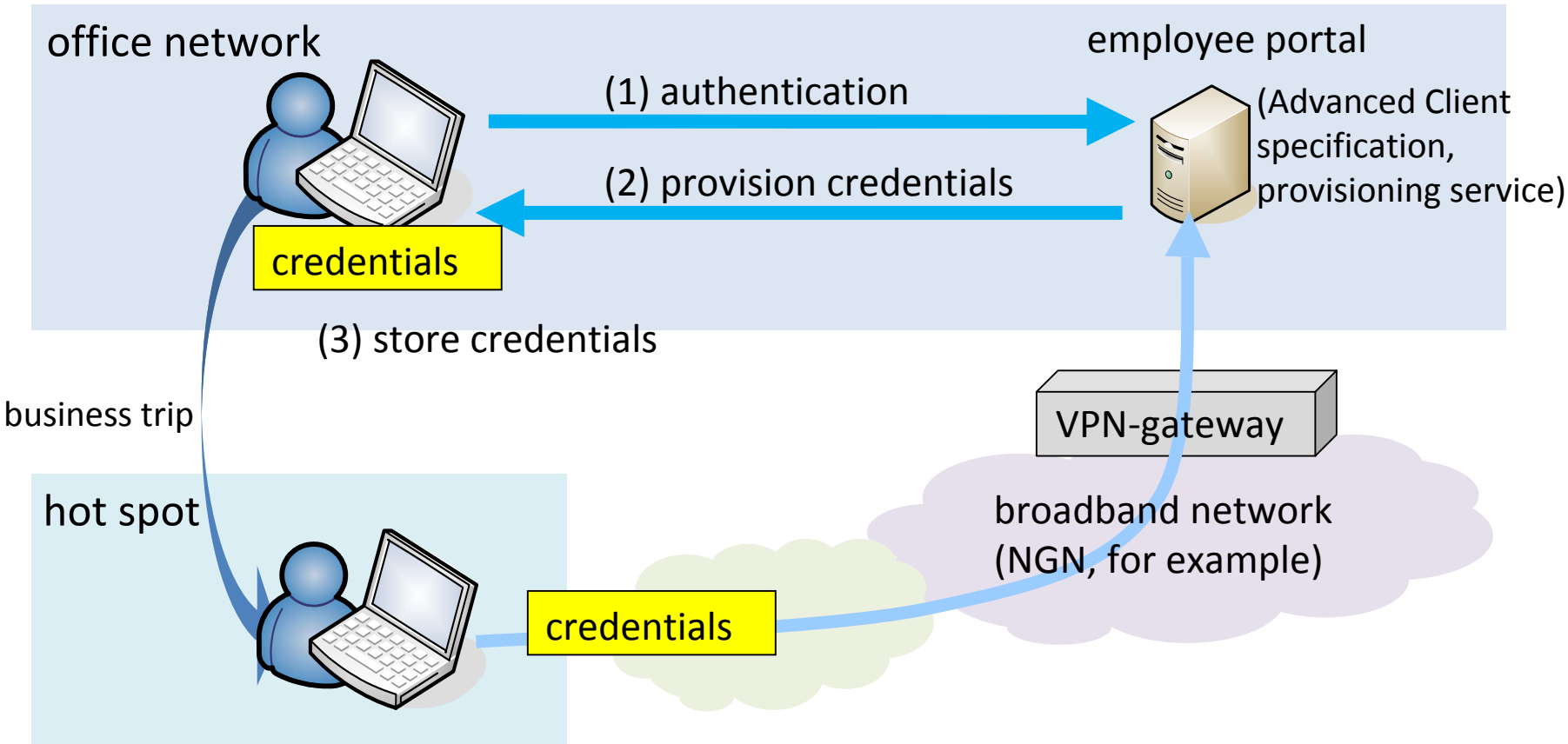
Separate credential container from Windows environment
Malware can not access credential container



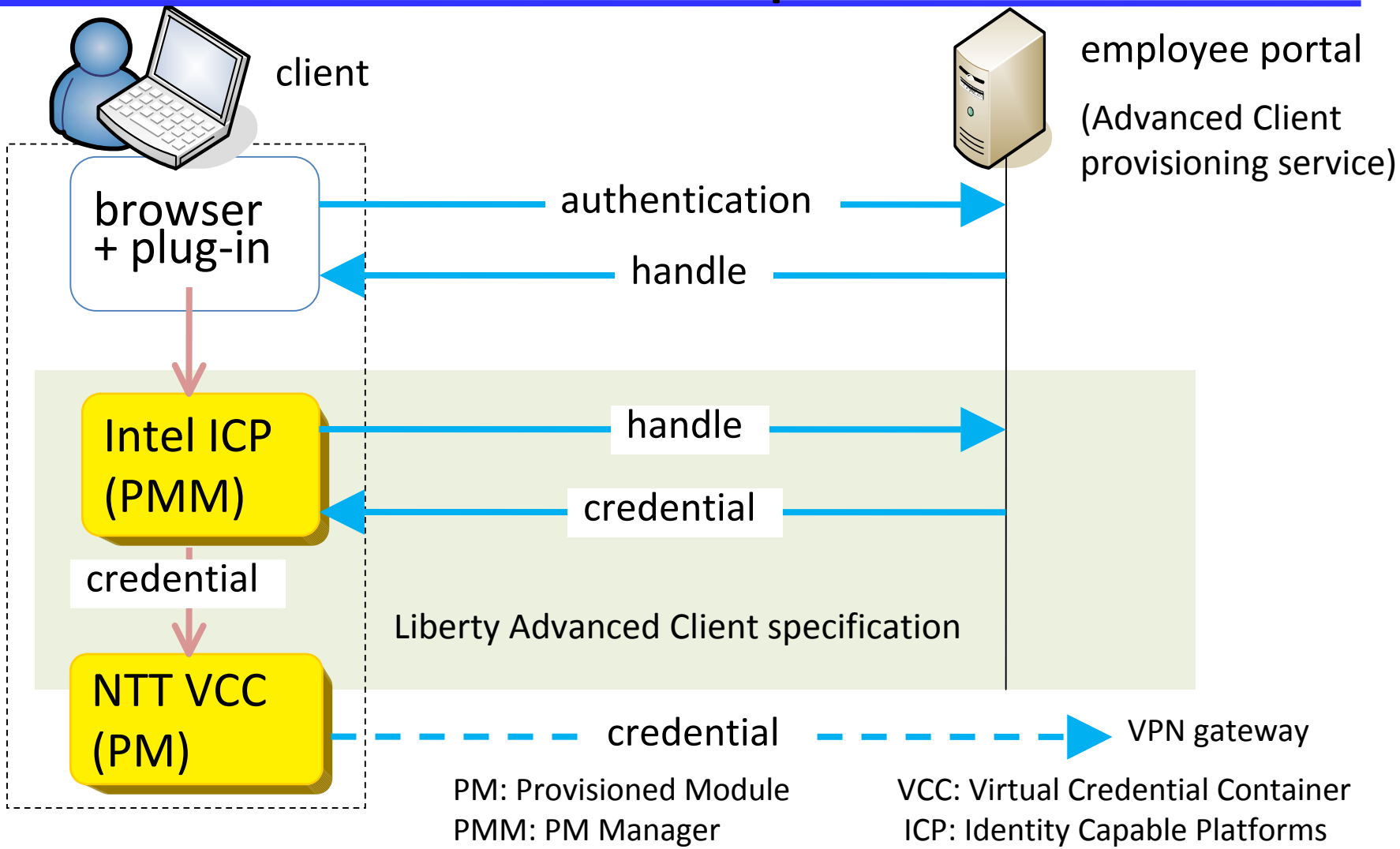
*: supports Microsoft Crypto API and PKCS#11

Use case: remote access scenario

remote access credentials are provisioned and stored securely to laptop located at office



Provisioning sequence based on Advanced Client specification



Issues: Countermeasures against laptop theft (T2)

- A malicious user detaches hard disk and reads credentials ⇒ Do not store credentials as plaintext

- Software encryption

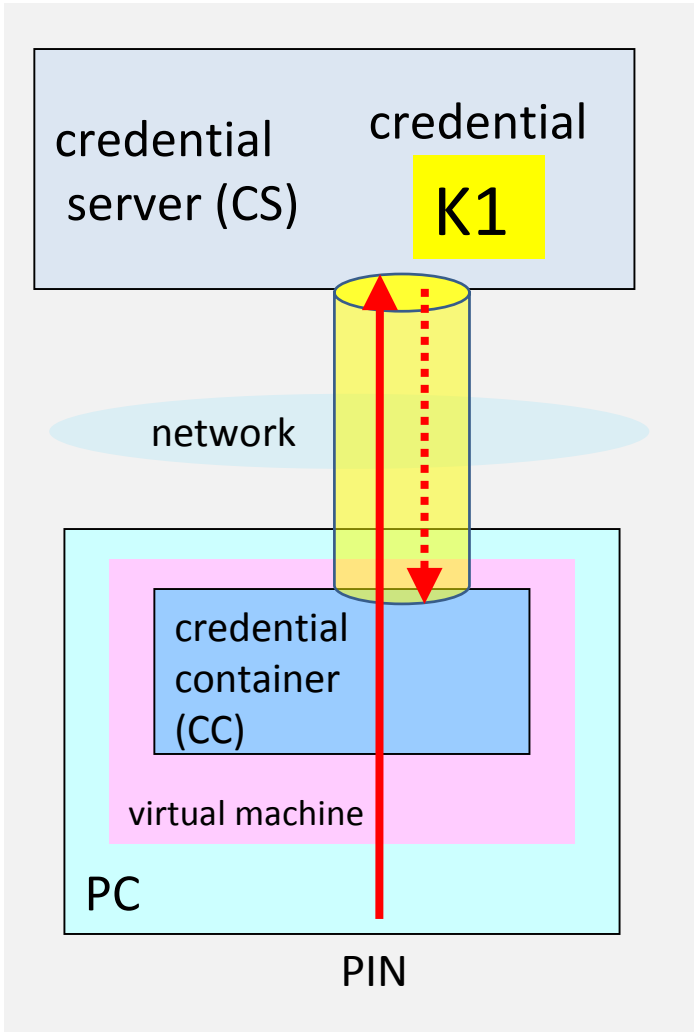
  Examples: Microsoft BitLocker, EFS

- Special Hardware

  Example: hard disk with full disk encryption

- Deposit credentials with a credential server, and download credentials on-demand

Deposit credentials with a credential server



Initial settings:
Deposit credential K1 with a credential server.

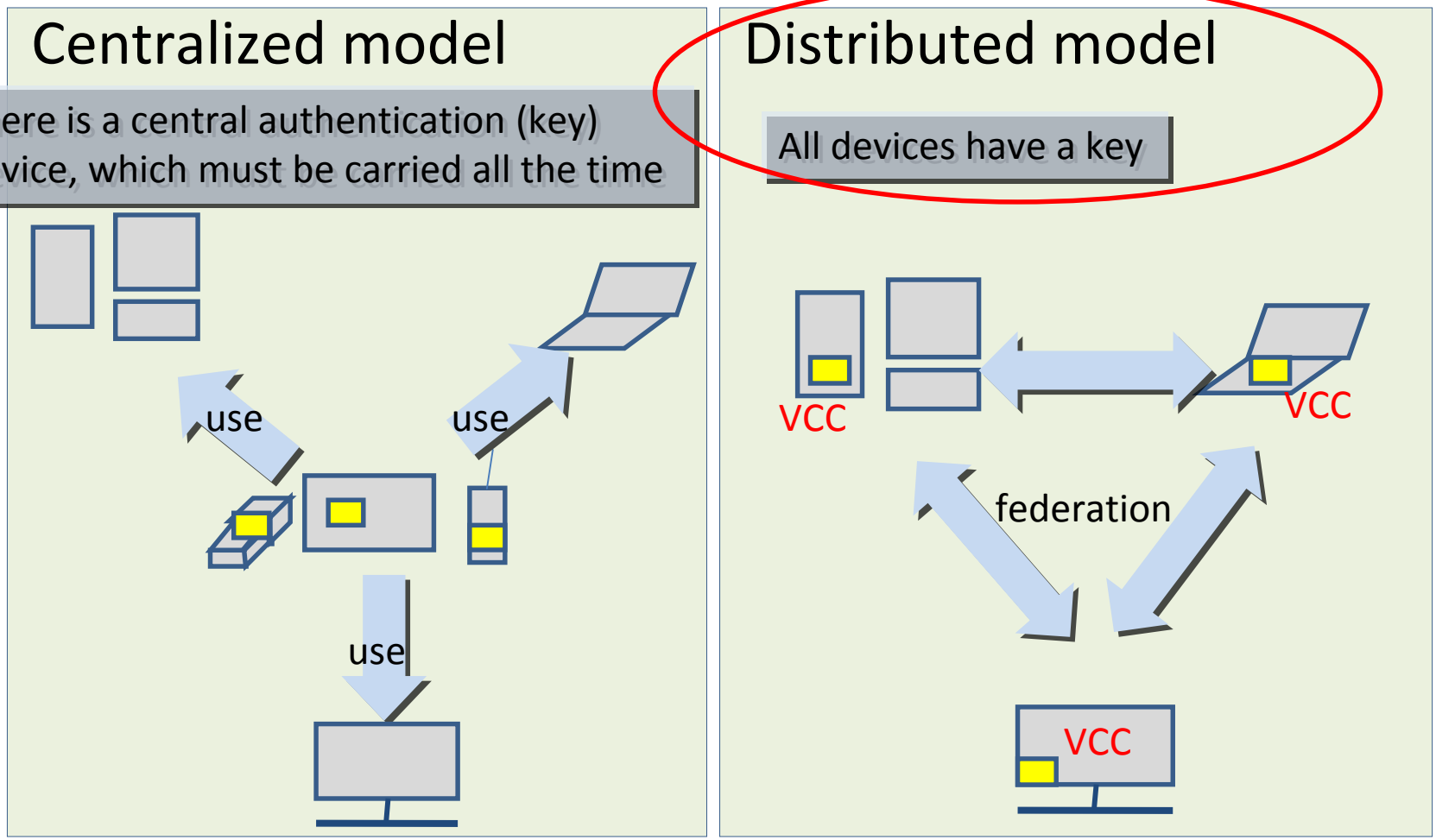
Download:
A user inputs PIN at the credential server, then credential K1 is sent to a credential container.

Security of virtualization

- We expect less vulnerability in VMM than that in OSs because the code is smaller
- Several threats related to virtualization have been reported
  - Example: virtual machine based rootkit, subsystem as spy problem
  - However, there are countermeasures
- From the technical point of view, there is no serious obstacle to the security of virtualization

Usage model of virtual credential container

Multi-device (ubiquitous) environment: a user wants to be able to use a service equally from various devices ⇒ requires relationship management among devices



Future works

- Explore more uses cases
  - SaaS (Software as a Service)
  - Fully converged Next Generation Networks
- Enhance manageability functions
  - Monitoring, updating, and deleting credentials (and programs that manage and use them)
- Adopt technologies to a wider variety of clients
  - Smart phones
  - Information appliances
  - Home gateways

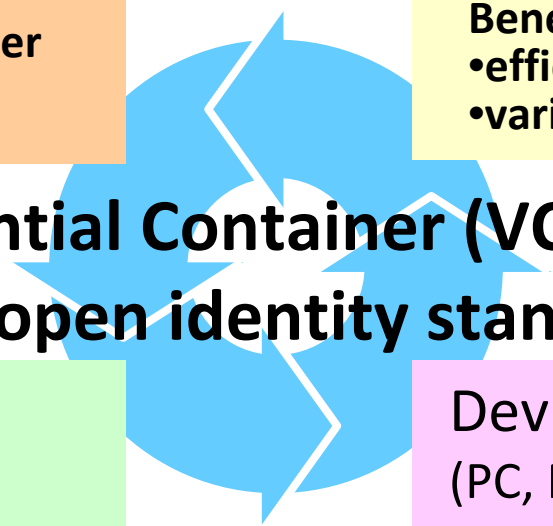
Towards secure credential ecosystems

Service providers
(SaaS, ASP…)

Benefits
•lower cost of and shorter time to deployment
•prevent illegal use

Network operators
(BB, Wireless, VPN…)

Benefits
•efficient provisioning
•various network usage



Virtual Credential Container (VCC) technology with open identity standards

Enterprises
Consumers

Benefits
•security
•lower cost
•convenience and confidence

Device vendors
(PC, Mobile, Software…)

Benefits
•advanced security
•increase customer loyalty

Contact us for more information: ufo-vt@lab.ntt.co.jp

Summary

The demo prototype consists of

- NTT Virtual Credential Container (VCC)
  - stores credentials securely for remote-access
- Intel Identity Capable Platforms (ICP)
  - provision credentials based on Liberty Advance Client specifications
- The solution will bring:
  - Significant cost reduction and greater client manageability to network operators, service providers, and enterprises
  - Convenience and confidence to users