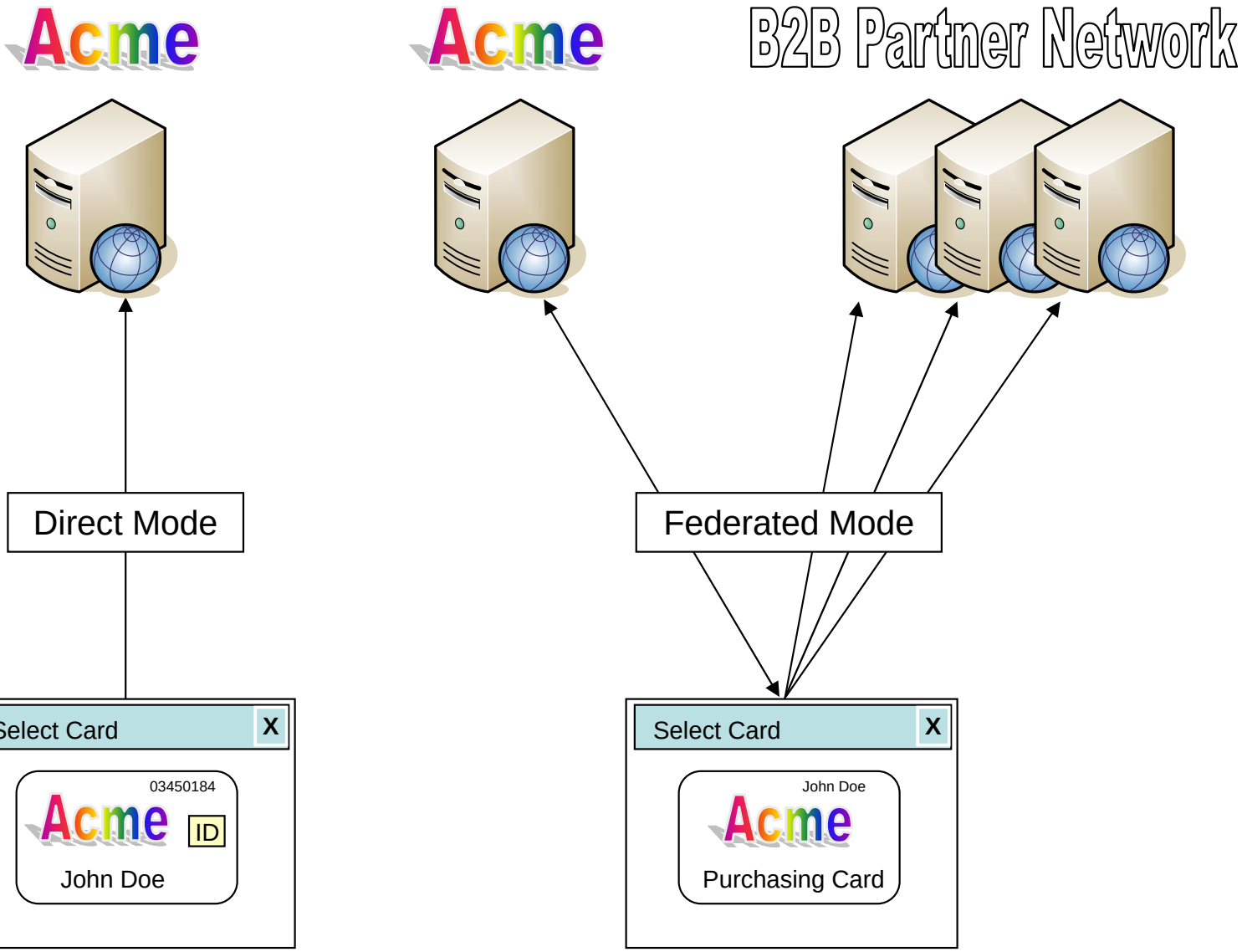
Two-factor Authentication in the Enterprise

It is sometimes claimed that a single enterprise credential can cover all authentication needs of an employee. This has in practice shown to be fairly theoretical for reasons like technical limitations in the infrastructure outside of the enterprise (a smart card typically doesn't work in public terminals) to privacy reasons (merchants do not really need your company or government ID, they rather need a *verified binding to the purchasing organization* or simply *a valid payment*).

Currently two-factor authentication schemes like OTP, PKI, and more recently Microsoft's CardSpace® are handled by completely *disparate issuing, distribution, and usage processes* making it difficult for organizations deploying multiple credentials addressing the situation described above.

This presentation outlines a "united" enterprise multi-credential vision in part based on a work-in-progress called KeyGen2.

One GUI Paradigm* - Multiple Credentials and Scenarios

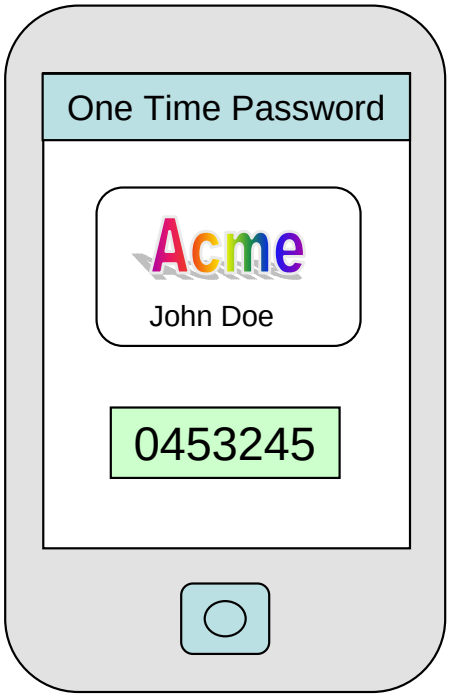


*) Client-side PKI in TLS can be regarded as managed cards running in self-issued mode

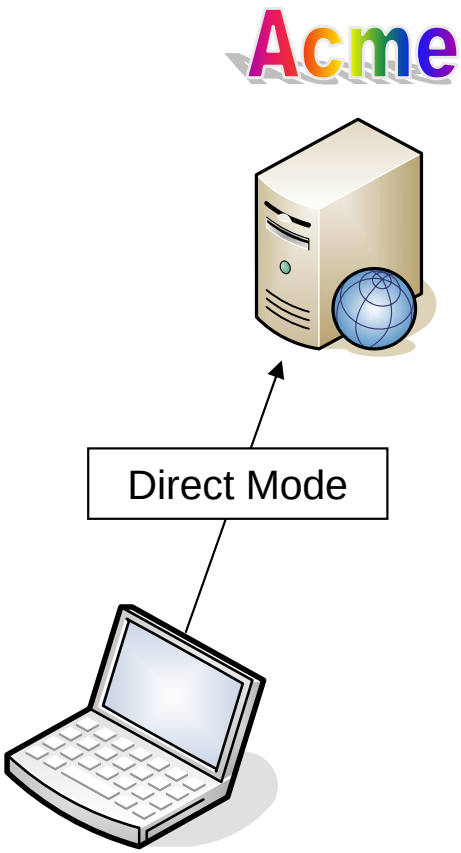
Enhanced TLS or Kerberos client using PKI for authentication to the Acme intranet

Information Card using PKI for authenticating to the Acme IdP

Ubiquitous Enterprise Web Access - An OTP “Killer Application”



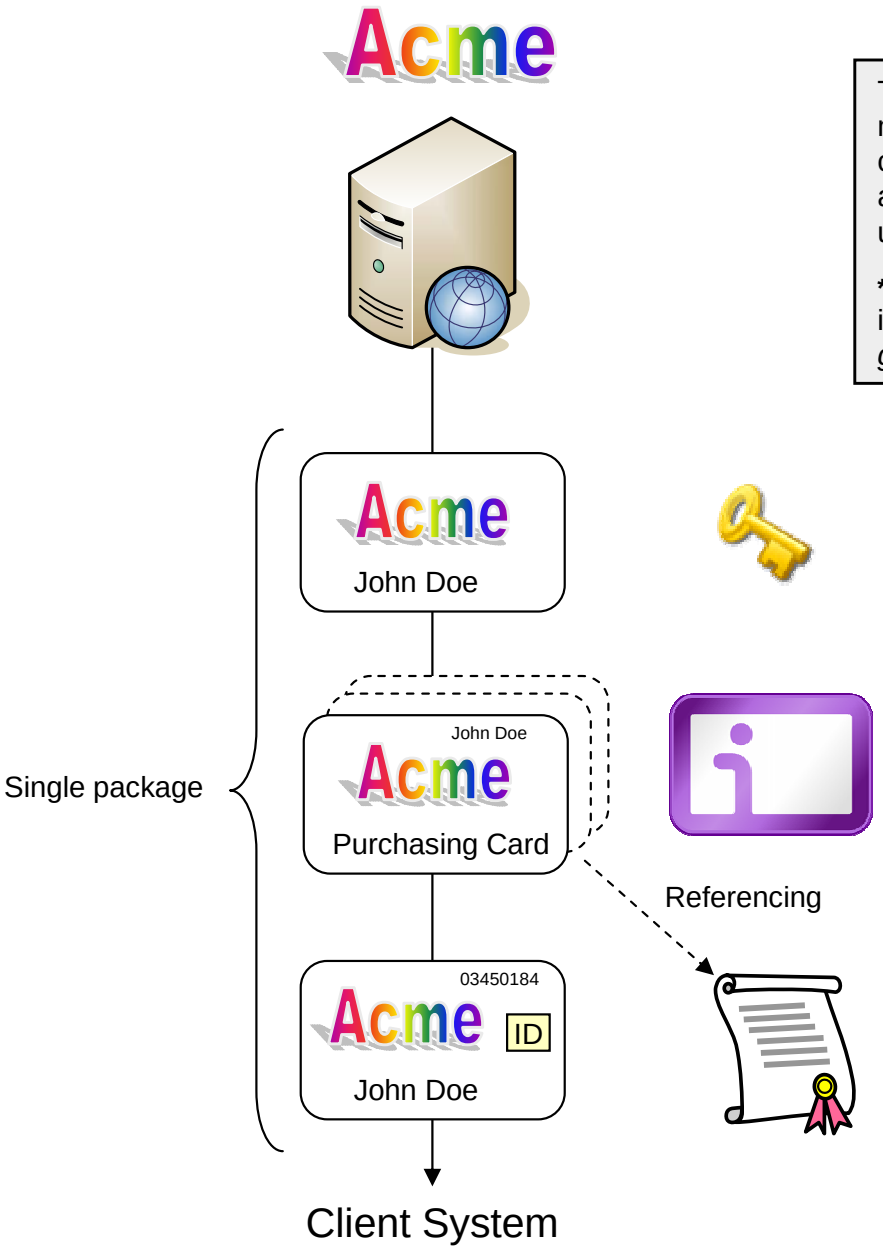
SmartPhone with OTP application support,
“emulating” OTP token devices



Standard “PC” (Windows, Linux, Mac)
without any additional authentication
middleware or hardware

Although not shown, OTP token selection can be performed using an Information Card GUI as well

One Provisioning Step* (using KeyGen2) - Multiple Credentials



The ability for an entity to issue and *manage* all user credentials “in parallel” makes it realistic offering multiple credentials, each optimized for a set of use-cases. To further reduce help-desk support and increase user-convenience, all credentials from a specific issuer would *typically* be protected by a single user-defined PIN.

*) From user’s point of view it appears to be a single step while the protocol itself performs 6 to 8 different passes, *including asymmetric key-pair generation in the client*.

OTP (One Time Password) “seed”

The card logotype was added for supporting an Information Card compatible OTP selection GUI

Managed Information Card(s)
You may need multiple cards, where each card is adapted for a particular federation network

PKI (primarily used for desktop and intranet login)
New usage: powering enterprise Information Cards
Potential usage: internal signature operations

The card logotype was added for supporting an Information Card compatible PKI selection GUI

And in *What* Should We Keep All these Credentials?

Maybe these guys are on to something?

http://middleware.internet2.edu/idtrust/2008/slides/03-pekka-roaming-identity.ppt