



Keynote: The Future of Data Leakage Prevention

ISSS Zürcher Tagung 2010
1.6.2010, WIDDER Hotel, Zürich

Sandy Porter

Head of Identity and Security, Avoco Secure

Data Leakage Prevention – The Future

Sandy Porter

Head of Identity, Security and Strategy at Avoco Secure

**Ensure only the
right people can
access and
use your data**



Copyright 2010

Data Leakage Prevention has been around for sometime...

- The UK military articulated the problem in an interesting way:
 - During the cold war we assumed that the second data has been created it will be stolen - What can you do?
 - Protect data at inception and link it to multiple authentication and identity.
 - Put the access controls/permissions in the right hands
 - No to the data administrators
 - Yes compliance, legal etc...

Data Leakage Prevention has been around for sometime...

- The military have Hundreds of thousands of users in de-perimeterised environments.
 - This requires an untethered architecture that dynamically protects data wherever it resides and can easily integrate/enable different systems.

How you protect your valuable Information is simple and makes sense.

- Encrypts the contents you wish to protect.
- Authenticates who can access that content.
- Controls what the recipient can do with that content.

So why not just do it if it is so easy?

Data leakage - issues

- DLP products basically stop at the perimeter and so address only part of the problem.

So the failure to prevent the major recent leaks in the UK civil government and businesses should not be surprising.

- You cannot control your client/partner end points etc...
- Which means building a new authentication system, co-opting users into it. It is limited also in its ability to apply policy as it is not an ID system.
- Next level up is Rights Management.
 - The issues of deploying complex tethered licensed server systems which also have significant issues beyond the perimeter.
 - Functionality of no print, no copy etc...is of limited value if the wrong person accesses the data in the first place.

Data leakage - issues

- DLP products and Rights Management in the future?
 - Complementary deployment – Yes the add value.
 - Direct integration – Many issues and of limited value in the new world.
 - What is missing from a combined offering is try linkage to identity and policies associated with each individual or organisation.

An Example of extending DLP products with Protection Settings for a strong Rights Management product.

- No copying content should include:
 - No third party screen capture
 - No access of content in memory (e.g. WinHex)
 - Watermarking with the person and organisation information.
- No printing content
- Audit
- Track the location of data
- Read Only
- Access controlled by multiple identities and identifiers.
- Date restrictions:
 - No access until
 - Expire after
 - Watermark

Data leakage - issues

- Data is now in a de-layered and de-perimeterised world today.
- Insiders and outsiders unauthorised access to information is an even higher risk now.
- Top of the Jericho forum agenda is secure collaboration. It is a must and achieving will add real value.

Enabling Secure collaboration

- Controls access to, and use of, documents based on identifying/authenticating a user.
- Permit documents to be restricted by location.
- Allows usage of content to be restricted *e.g.* copying, printing, date restrictions, use in virtual machines, *etc.*

Trusted sharing of confidential information

- In the De-perimeterized world and future Clouds, data must be considered in a new way and how you protect it has to change.
 - Previously static data that did not get disseminated.
 - Data is now dynamic in an environment encompassing distributed computers and distributed users.
 - In this environment, the ability to link dynamic security **policies** to **identity** and **information** is a key enabling factor in creating solutions that will persistently secure and control that information.

The components required to successfully protect encapsulated data going forward:

- The data itself being viewed as a “nugget” and the protection being an inherent part of this, to create a secured data package.
- This secured data package being un-tethered (independent) and so retaining the natural fluid movement that is a defining aspect of unstructured data.
- Directly linking an identity or identities to the secured data package – setting a policy of belonging to (policy linkage).

The components required to successfully protect encapsulated data going forward:

- Driving the protection of the data package using policies.
 - Applied automatically at any point in the data cycle.
 - That can be changed dynamically on demand.
- Applying an additional layer of controls to the use of the content after access to assure integrity.
- This linkage ensures that even if re-directed, accidentally or maliciously, or taken out of residence, access to the content will be prevented without the correct access token.

The components required to successfully protect encapsulated data contd:

- These elements, built into the process of retaining data, will ensure privacy of the information due to a culture of 'belonging to...' built into the system:
- The security of the data is determined by the encryption and controlled access.
- The integrity is assured by the post access content controls.

*Identities, dynamic policies and claims being utilised to enforce **where, when, why, who** and how data can be accessed.*

Identifying Users in the De-perimeterised World.

- New types of digital identity are being developed.
 - Follow the model of geographic / location independence and user centricity.
- More liberating than existing desktop/device based methods (e.g. Smart card certificates).
 - But can utilise these systems to add security.
- Examples are User Centric Identities including OpenID initiative and Information Cards.
 - Information Cards can act in both desktop and Cloud domains
 - Issue around security for OpenID.

Identity and Policy

- Leverage **identity** and **policy** by the use of multiple authentication and dynamic claims to access and control content contained in files.
- Revoke an identity and an individual ceases to have access to the documents wherever they reside.
- I cannot revoke a national or third party's identity.
 - Create a user centric identity like an information card and you can control the revocation of the card or dynamic claim.
 - Or rather than revoke an identity, associate a dynamic claim with an I-Card which can be changed in real time.
 - An Audit Information card can be used to revoke access to email, documents and other resources.

Information Card Identity

- Are a digital representation of the real world you and they contain:
 - Claims and Credential which belong to you and can be almost anything.
 - They can be verified by third parties.
 - Third parties can supply verified claims.

Information Card Identity

- Selectable verification includes X509 digital certificate, voice biometric, I-Cards etc....
- Custom dynamic claims may be added e.g. user security clearance level, reputation rating (1-10 star), credit agency, passport office, driving license, National ID...
- Supports instant revocation of either claims or the cards themselves to revoke or change access rights.

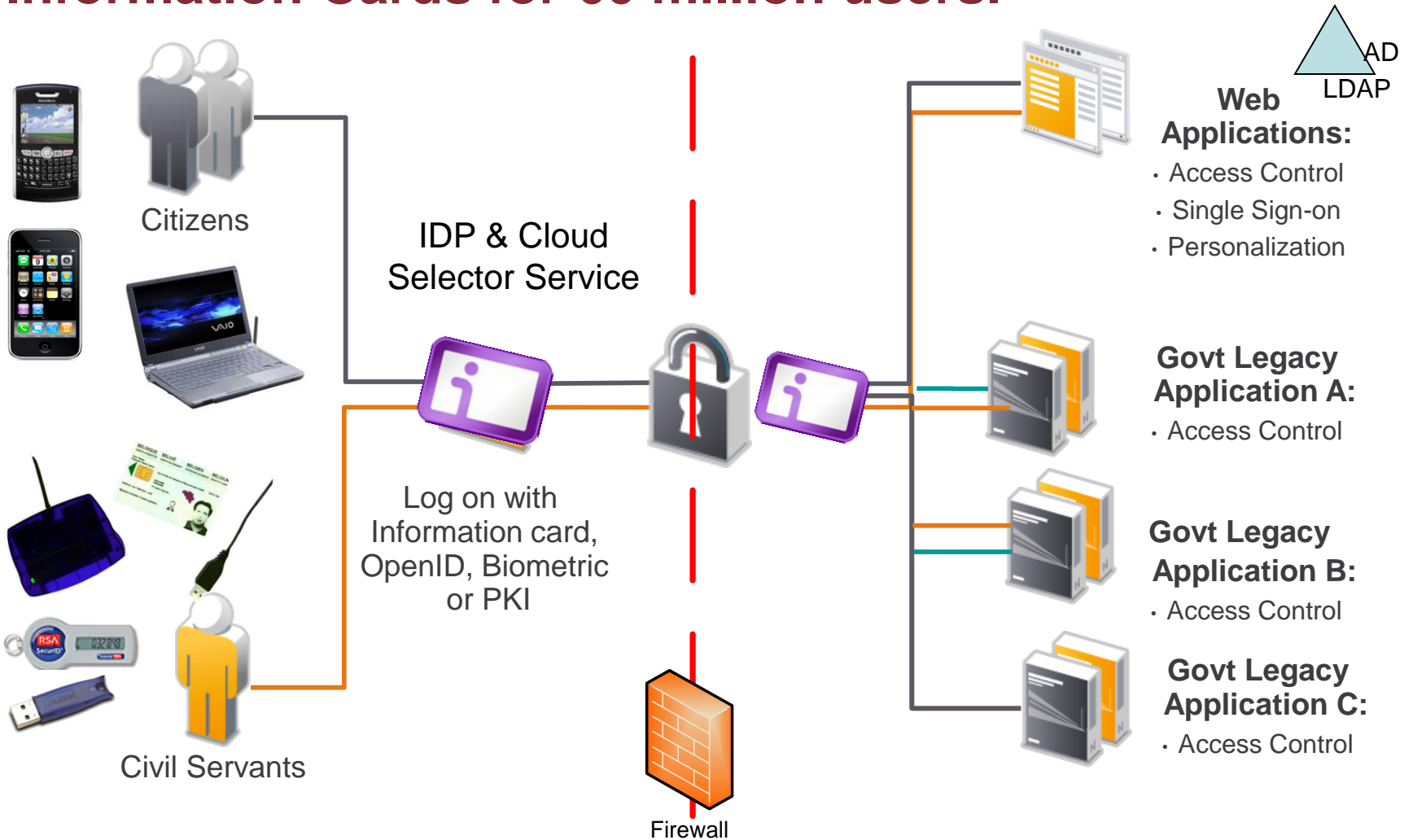
Offers: Privacy, Security...

- Users and providers can specify which I-card may be used, when, and how and where.
- Users can control the information supplied to third parties.
- Dynamic claims can be associated with the use of each identity.
- Takes the best of credit cards, PKI and user name password models.
- Simple to use, low cost and ease of deployment.

New thinking and how claims add value

- Wherever possible, we believe that personal data should be controlled by individual citizens themselves. – *New UK Government*
- Bi-directional Trust can increase security and reduce liability.
- People are able to see and control what they share.
 - Education of users and ensuring only the right data is shared when required are benefits.
 - DLP policies can now easily be associated and applied via user centric identity claims.

An example of the first stage we are looking at for a customer: Cloud Selector Service and Managed Information Cards for 60 million users.



Location

- Where data is accessed is becoming more relevant.
 - Online services and the Cloud.
 - Regulatory and privacy requirements.
- An example of applying location control.

Choose your location

GPS Settings

Description: The White House

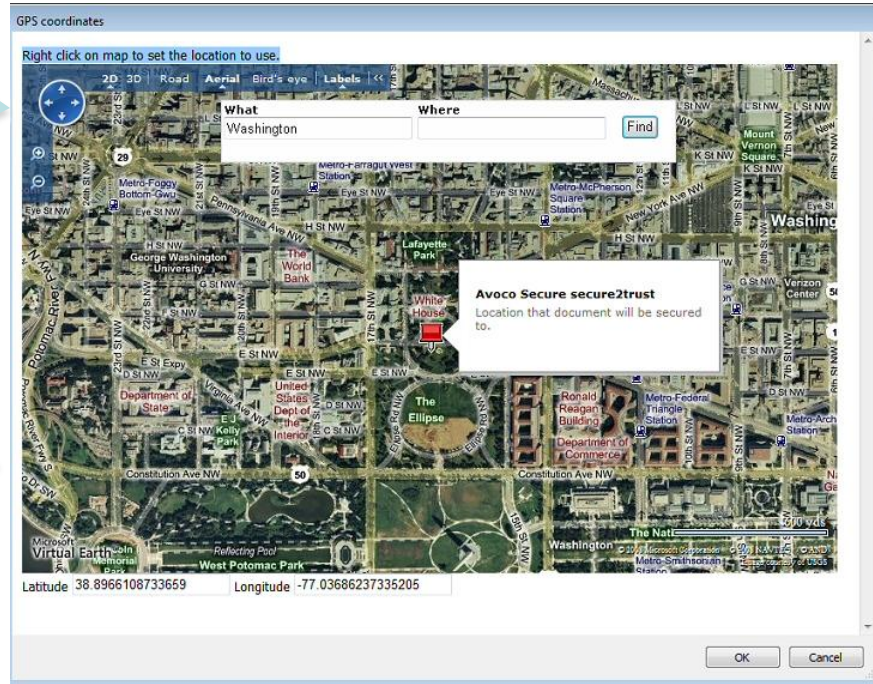
Location

Latitude: 0.000000 Pick from postcode, location or map

Longitude: 0.000000

Allowed tolerance (metres): 0 M

Access code:



Once your location coordinates are set you can then say what can be done with the document after access

GPS Settings

Description: The White House

Location

Latitude: 38.8966108733659 Pick from postcode, location or map

Longitude: -77.03686237335205

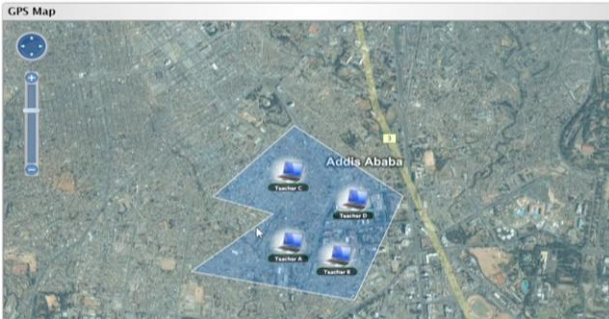
Allowed tolerance (metres): 30 M

Access code: 123456

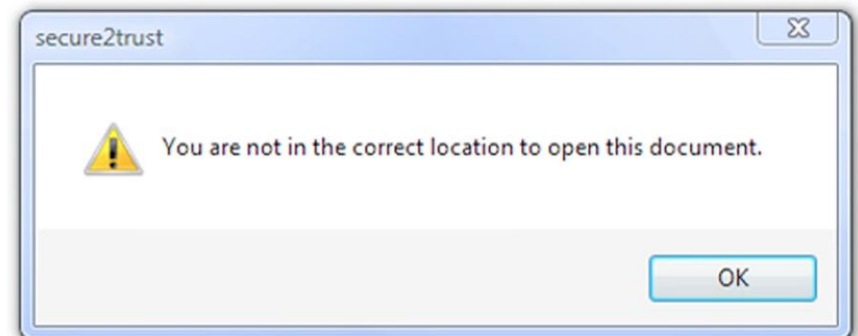
Can be combined with any of the other access control mechanisms to add additional layer of authentication

Location aware Data in a De-perimeterised World

Location aware data can be tracked and actions on it audited inside and outside the “zone”.



The movement of the data is being tracked and when it is outside of the access zone will not open.



The Cloud is an Opportunity and not just a Risk

- Because of the real-time nature of online or Cloud based applications, policies associated with content in the Cloud can be changed at any point, and automatically updated to reflect that change.
 - This provides powerful workflow control.
 - This will enable highly granular control.
 - Identity services can be hosted.
 - Dynamic claims services online accessed in real time.
 - This extends DLP beyond the perimeter.

The Future

Content (information) centric based approach to security

+

Information Card (User centric and friendly)

+

Multiple Authentication (More secure)

+

Geographic Location (Greater control)

+

Live Tracking (Audit and traceability)

=

Enhances Security in a De-layered Network and De-perimeterized World.

Thank you



Sandy Porter

sandy.porter@avocosecure.com

+44 (0)791 750 7636

www.avocosecure.com

Data in motion - which may be located anywhere – needs security linked to user centric identities and dynamic policies- that are seamlessly applied to your information.

© Sandy Porter 2010