

# **EHerkenning**

## **Dutch eRecognition (eHerkenning) Pitfalls creating an eRecognition Trust Framework**

**1 December 2011**

**Kick Willemse**

**k.willemse@evidos.nl**

**+31 627006866**



IRVING BERLIN

# THERE'S NO BUSINESS LIKE

DIRECTED BY  
WALTER LANG

PRODUCED BY  
BOB C. SIGGEL

© 1941 MCA, INC. ALL RIGHTS RESERVED.





# e-Government

# EHerkenning

How do we recognize our online customer?



*"On the Internet, nobody knows you're a dog."*

Various Dutch market parties and leading governments have combined their forces in a set of agreements facilitated by the government (TrustFramework)

Consideration for shared topics, including:

- ❖ user experience
- ❖ quality
- ❖ information security
- ❖ technology
- ❖ control

Preconditions set by the Dutch Ministry of Economic Affairs, Agriculture and Innovation, including:

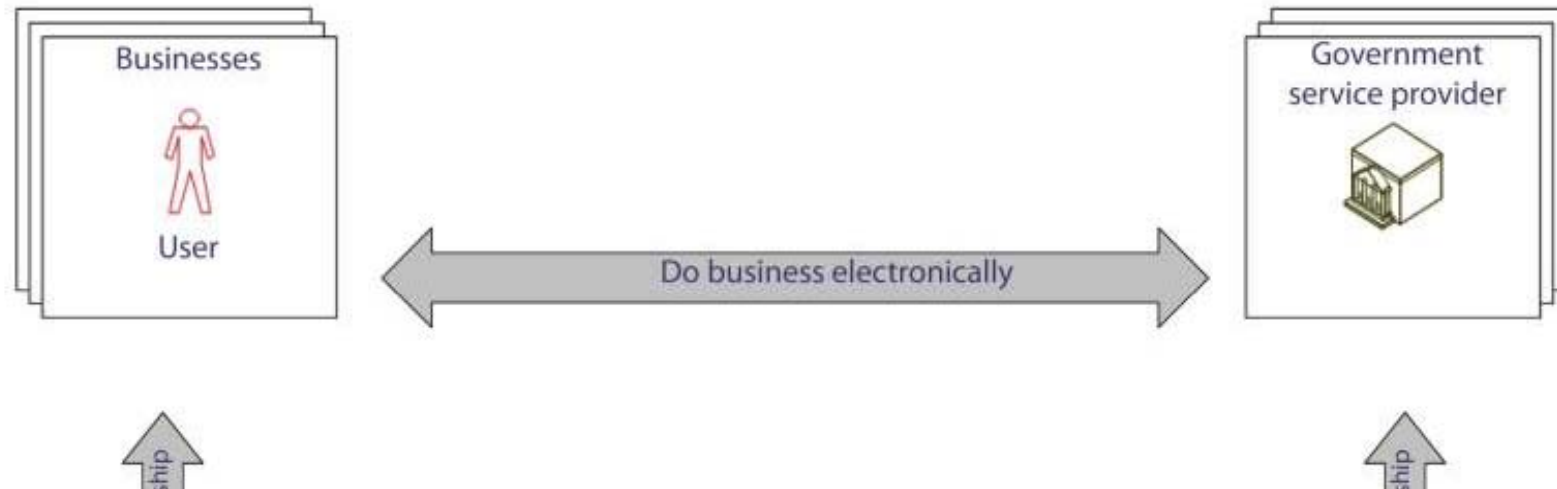
- ❖ 'the market works it, unless...'
- ❖ collaboration regarding common topics
- ❖ competition



# EHerkenning

## eRecognition Trust Framework

A service for digital recognition of businesses





## BEDRIJVEN >>



### Eenvoudig en betrouwbaar gegevens uitwisselen met de overheid

eHerkenning zorgt ervoor dat de overheidsorganisatie waar u inlogt uw bedrijf direct kan herkennen.

[Meer informatie >](#)

eHerkenning aanvragen >

## OVERHEDEN >>



### Efficiënte en betrouwbare elektronische dienstverlening

Dankzij eHerkenning weet u als overheidsorganisatie direct met welk bedrijf u te maken heeft en of de handelende persoon gemachtigd is.

[Meer informatie >](#)

eHerkenning aansluiten >

## Wat is eHerkenning?

eHerkenning regelt dat bedrijven zich digitaal kunnen identificeren wanneer ze elektronisch zaken regelen met de overheid. Dat doet eHerkenning op een efficiënte, betrouwbare en eenvoudige manier.

Overheden weten dankzij eHerkenning met welk bedrijf ze te maken hebben en of medewerkers gemachtigd zijn om namens het bedrijf te handelen. eHerkenning heeft vele voordelen en toepassingsmogelijkheden.

> eHerkenning voor bedrijven

> eHerkenning voor overheden

## Nieuws

**04.08.11** De Gemeente Zwolle lanceert als een van de eerste gemeenten...  
[Lees meer >](#)

**25.07.11** De Kamer van Koophandel heeft sinds 1 juli het nieuwe...  
[Lees meer >](#)

**18.07.11** Aanvragen ingediend onder DigiD voor bedrijven niet terug te vinden...  
[Lees meer >](#)

> Meer nieuws

## Naar de demo



Nu meteen eHerkenning betrouwbaarheidsniveau 1 aanvragen >



## Antwoord voor bedrijven *Berichtenbox*

### Berichtenbox: inloggen of registreren

De berichtenbox voor bedrijven is een beveiligd e-mailsysteem waarmee u digitaal berichten kunt uitwisselen met Nederlandse overheidsinstanties. U krijgt toegang tot de berichtenbox met een gebruikersaccount van Antwoord voor bedrijven of met een eHerkenningmiddel.

> [Ik heb nog geen account / Geef mij meer informatie](#)



[Gebruik Antwoord voor bedrijven:](#)

- als u een gebruikersaccount hebt van Antwoord voor bedrijven;
- als u een nieuw gebruikersaccount van Antwoord voor bedrijven wilt aanmaken.

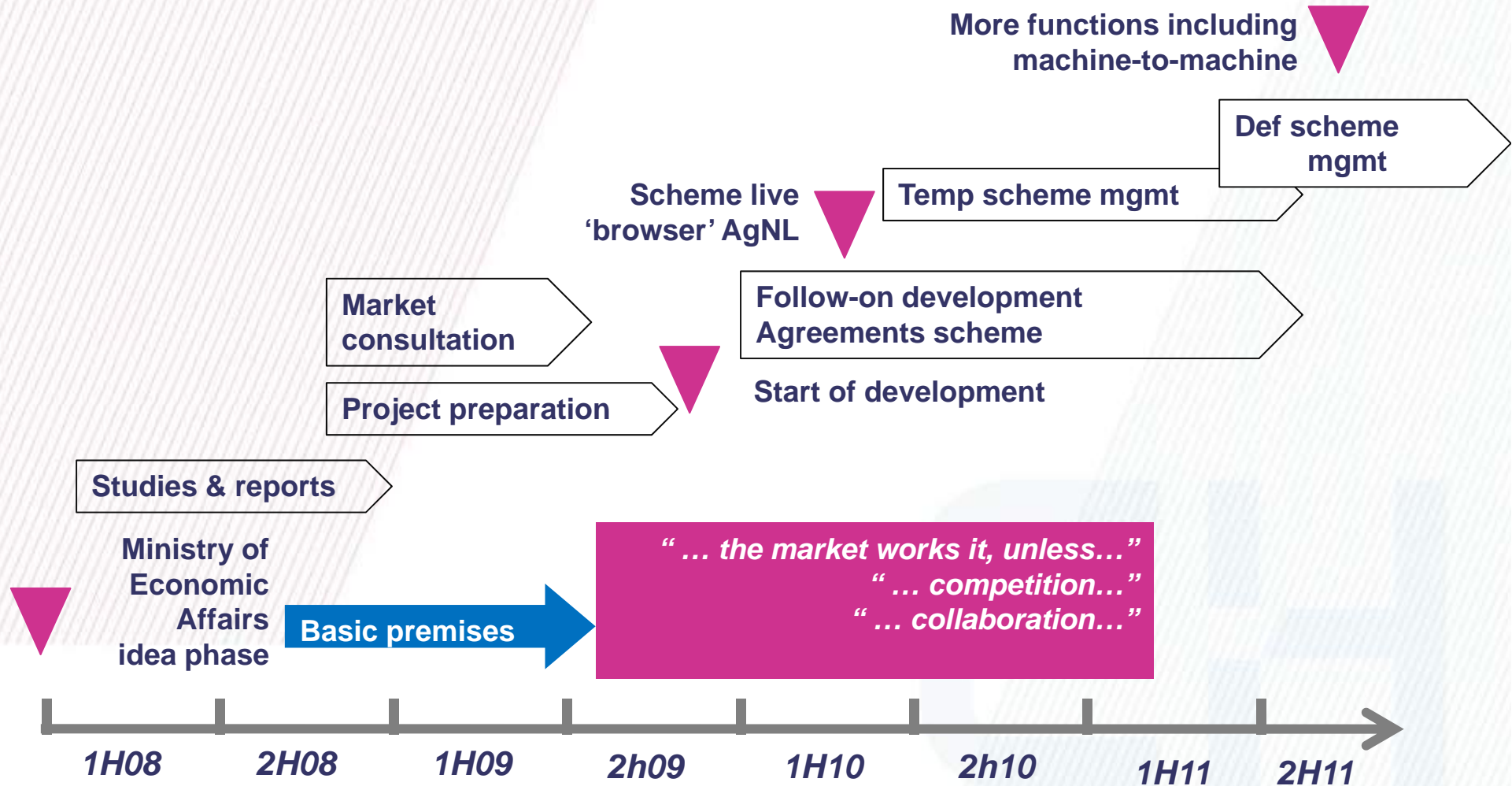


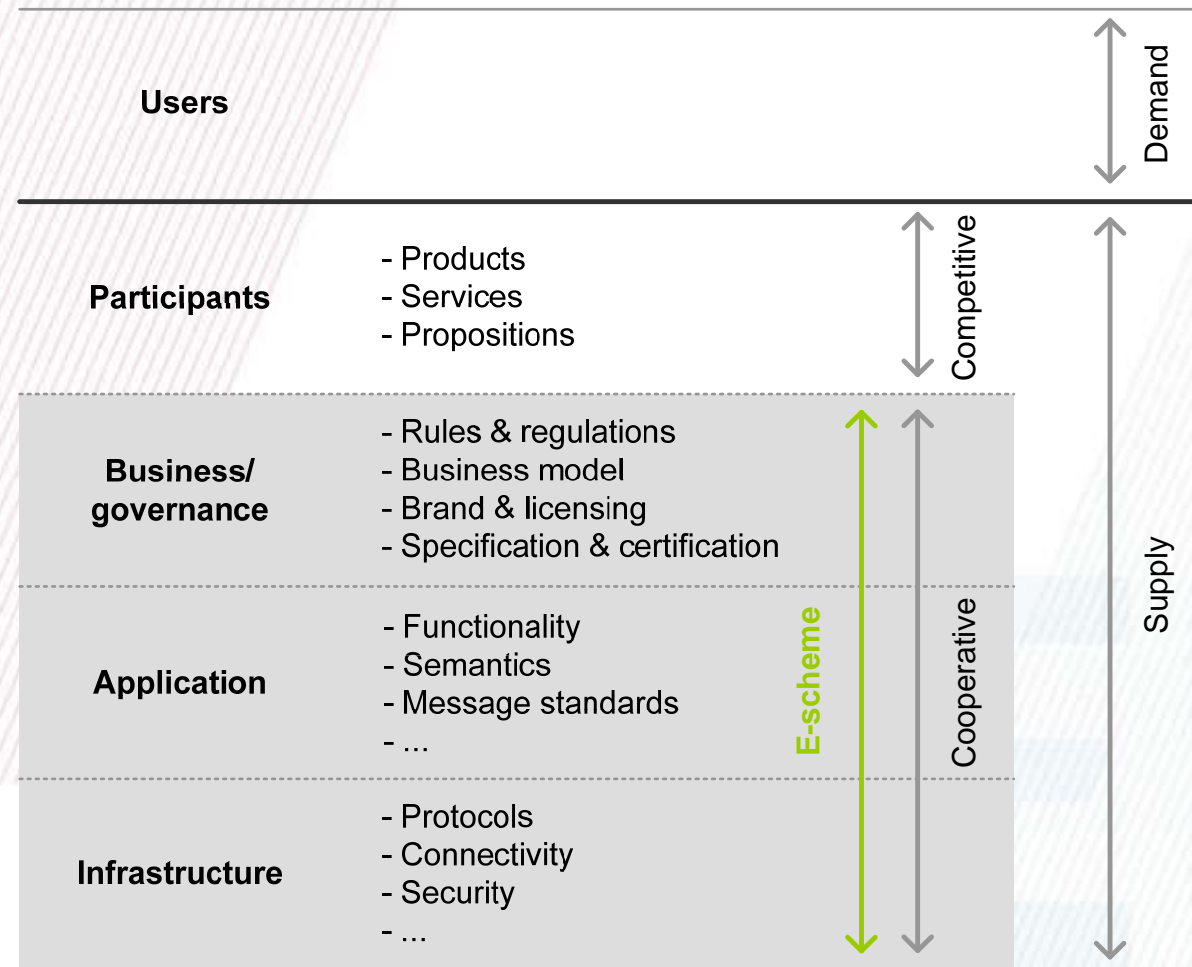
[Gebruik eHerkenning:](#)

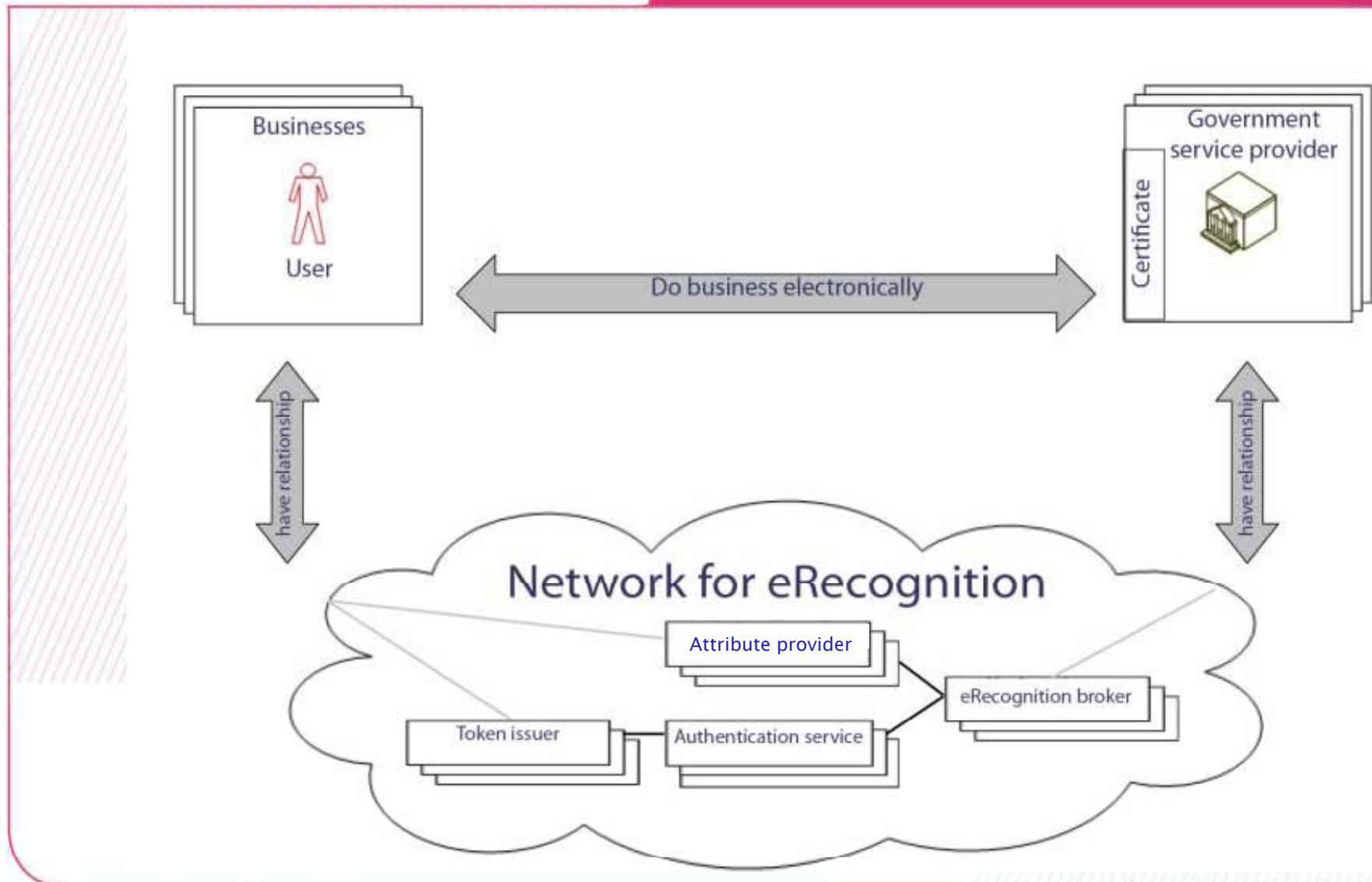
- als uw berichtenbox is aangemaakt met een eHerkenningmiddel;
- als u via eHerkenning gemachtigd bent om gebruik te maken van de berichtenbox van uw bedrijf;
- als u een nieuwe berichtenbox wilt aanmaken met een eHerkenningmiddel.

# EHerkenning

## Development of eRecognition



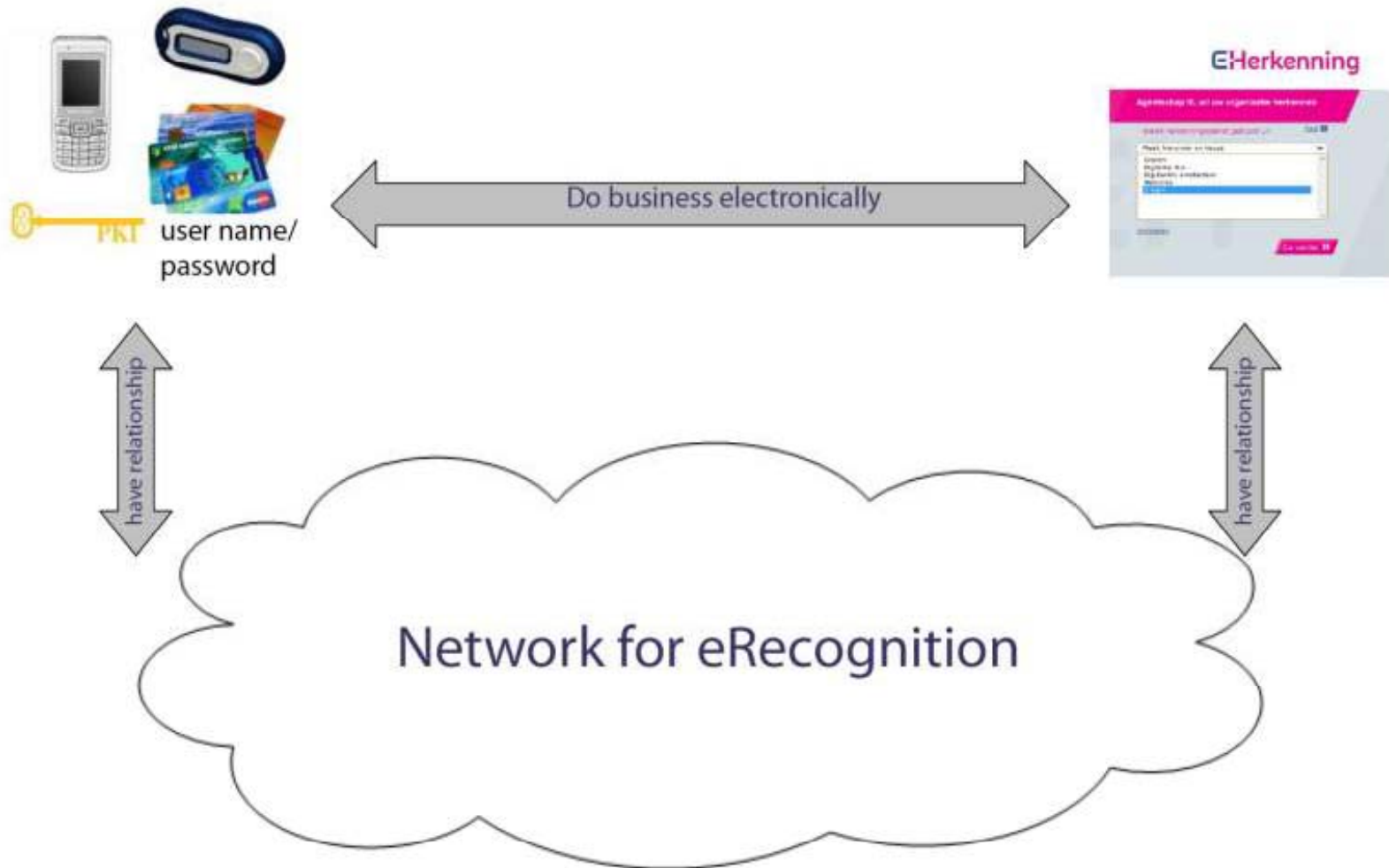




# EHerkenning

## Reuse of available tokens

eRecognition combines solutions available in the market into an uniform basic user experience



# EHerkenning

## Various assurance levels in one set of agreements

BETROUWBAARHEIDSNIVEAU



BETROUWBAARHEIDSNIVEAU



BETROUWBAARHEIDSNIVEAU



BETROUWBAARHEIDSNIVEAU







User name /  
password

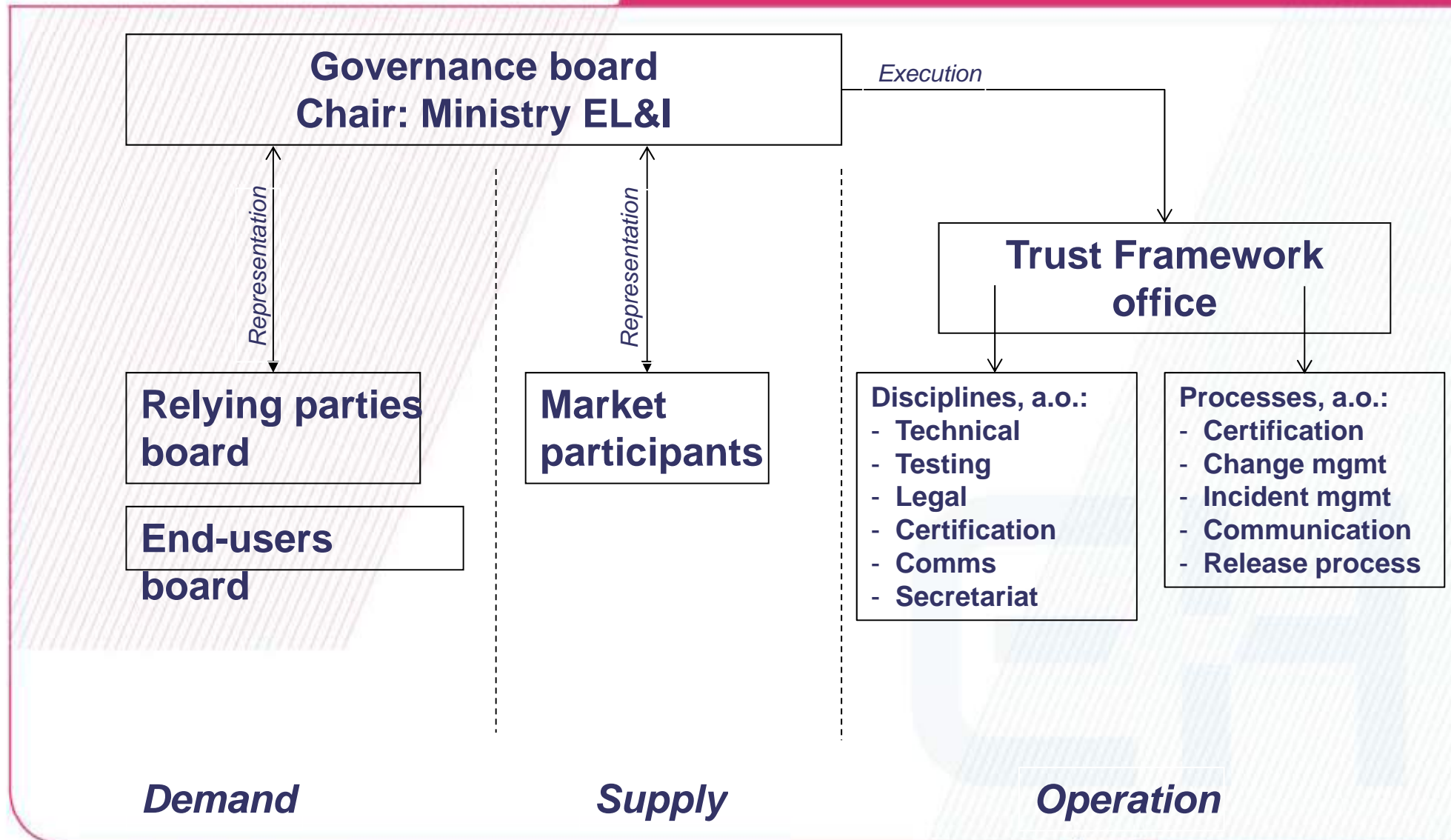


*The service provider's process  
determines which level is to be used*

# EHerkenning

## Various assurance levels in one set of agreements

Level		Registration process characteristics	Token characteristics	Application (example)
1 Minimal assurance		No or minimal control, email address at most Registration of association with the business on the basis of data, validated by Chamber of Commerce (CC)	User name and password	Contact form, notice of objection
2 Reasonable assurance without appearing in person		Validation of personal details by means of e.g. photocopy of identity card, bank transaction Authority check using CC data Reliable issue, e.g. by registered mail or verified email	2-factor (knowledge and possession): text message, one time password (OTP) token, certificate	Parking permit, catering licence, subsidy (limited volume)
3 High assurance		Validation of personal details by means of original identity card or compatible Authority check using CC data Reliable physical issue, e.g. by registered mail	2-factor (knowledge and possession): text message, one time password (OTP) token, certificate, bank card	VAT, income tax, subsidy applications (large volume)
4 Very high assurance		Validation of personal details by means of original identity card when appearing in person. Registration of authority necessitates appearing in person of at least the legal representative and, if applicable, the administrator	Qualified certificates on a safe solution (PKI level, conform Dutch Electronic Signature Act)	Changing national register data (e.g. CC), inspecting court data



- **Soft Launch in 2011**
- **Primary B-t-G, but B-t-B in progress**
- **15 market parties involved**
- **10 Gov services involved**
- **Tax registration is killer app, will launch 2012**
- **About 30.000 new credentials issued (Market 1 million companies)**
- **Re-Use of credentials, work in progress**
  - **Banks**
  - **Telco**
  - **National ID**

**Some potential pitfalls for full deployment in 2012...**

**.There is a strong discussion on who needs to take the role to issue credentials to end-user. Is this a task of the Government (National e-ID) or should we leave this to the market (Banks, Telco's)?**

### **Counter measure:**

- Take an Hybrid Approach and let the end-user choose**
- Both Public and Private credentials part of the trust framework**
- This will drive innovation and makes even more credentials available for re-use**
- Some attribute registers are managed by the government**
- Make sure there is a fair competition (no free id's by government)**
- Even large multinationals can join the trust framework with their corporate credentials**

**.The eRecognition Trust Framework is a 2 sided market like the mobile phone market and therefore characterised by the famous Chicken-Egg problem. There is big risk that the Trust Framework will never reach economic self sufficiency**

### Counter measure:

- During the growth stage, the trust framework needs financial support
- Stimulating the growth strategy should be as short and steep as possible to make sure:
  - End-Users will not loose momentum
  - Market vendors will not stop investing
  - Relying Parties will have trust in stability of the platform
- Stimulate financially end-user credentials and RP service development
- Promotion and education activities
- Interchange, transaction based within Trust Framework

**.80% of e-transaction volume goes via machine-2-machine channel and not via browser interaction**

**.First webportals see important change by having more mobile visitors than web visitors**

### **Counter measure:**

- Trustframwork should take m-2-m communications into account**
- M-2-M is not only PKI/ SSL based but for different LOA's credentials**
- Technical protocols should be able to handle mobile or m-2-m communications**

You have to manage credentials in a trust framework, it is not only about issuing a credential!:

- People loose credentials
- Relying parties will merge
- Market parties will leave the framework

### Counter measure:

- Be careful with pseudonyms correlation to the lifecycle
- Think about transferring credentials to another market party
- Promote the use of multiple credentials
- Describe lifecycle management In your trust framework



**.Credentials can be issued on a level of assurance, user attributes related to the credential can't. Attributes like e-mail, address, phone, name are verified or not.**

**.Attributes are an important value that is delivered by the framework**

**.Attribute scheme needs to be standardised**

### **Counter measure:**

- Work with technical protocols that support attribute exchange and user consent**
- Define method of verification of attributes, but not levels of assurance**
- Link attributes to a pseudonym credential**

It is not only about the trust in issuing credentials on a level of assurance. Trust Framework should also guard the trust within an operational framework.

### Counter measure:

- Relying Party's should have certain countermeasures in place
- CookBook for mapping LOA's to RP services
- Penalty's for Market Party's that do not comply, but beware; temporary revocation of licence is not an option!



**.An even bigger challenge after solving the identity trust framework; People are delegated to act on behalf of someone else.**

**.Is User X authorized to do Y on behalf of user Z?**

### **Counter measure:**

- Make it possible to delegate your credential to another user**
- Define a scope catalogue to have a list of services to be authorized for**
- Make it possible to register these authorization claims**



**.Trust Frameworks will cross borders!**

**Counter measure:**

- International Meta-TrustScheme
- International standards on technical interfaces
- Align Attributes and Identifiers



# EHerkenning

Thank you: Questions?

