ECMA

Standardizing Information and Communication Systems

Standards for Security in E-Business

Activities by ECMA TC36 (IT-Security)

Dr. Helmut Stiegler
STI-Consulting D-81245 München
helmut.stiegler@sti-consulting.de

ECMA

About ECMA

Formerly

European Computer Manufacturers Association

about 60 company members worldwide

”Facilitate and standardize the use of information processing and telecommunications systems.”

www.ecma.ch

ECMA/TC36 IT-Security

Scope

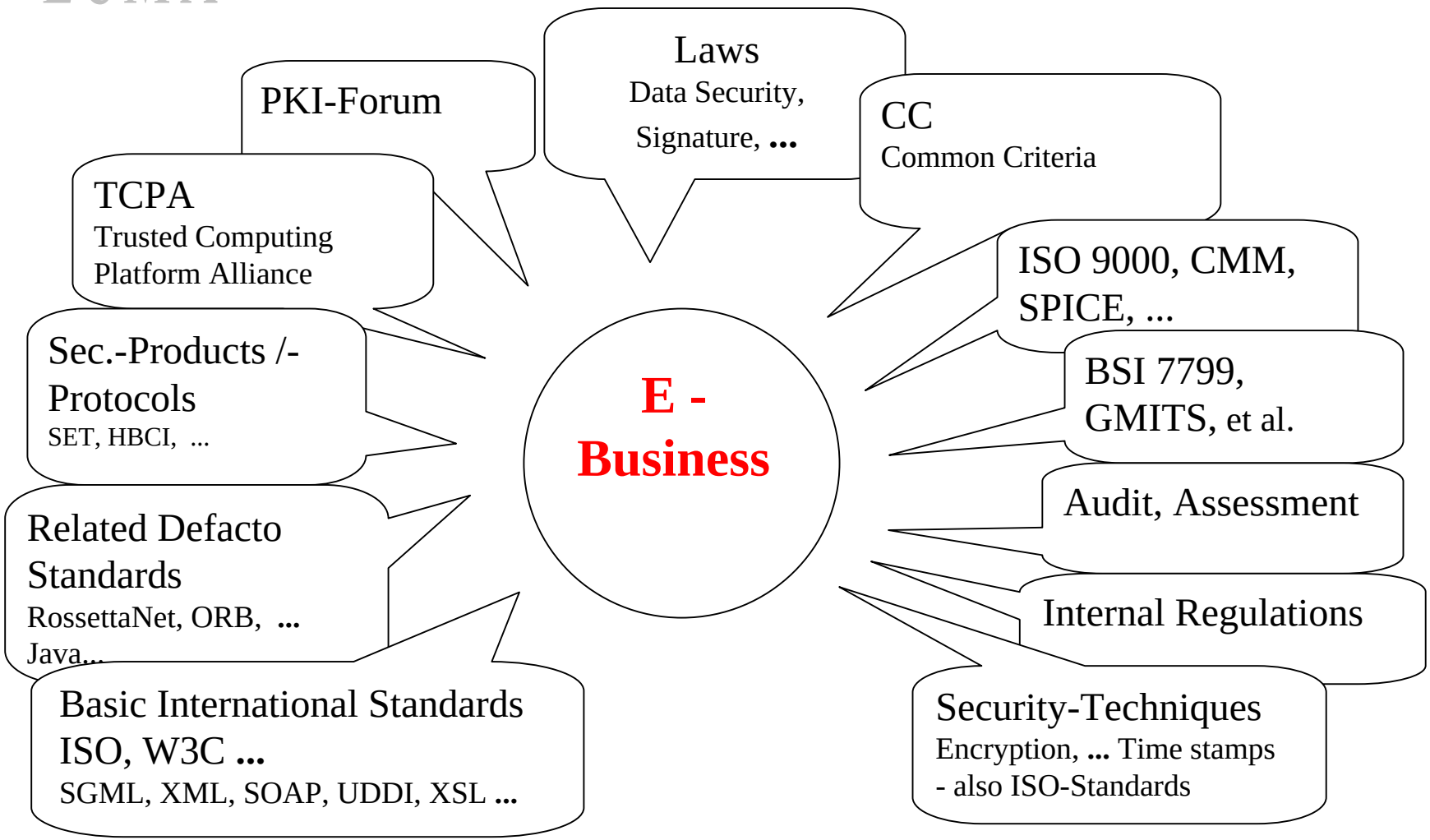
"To research standards and technical reports that promote appropriate IT security practices which enable the expansion of the IT market. Security practices include the IT security aspects of trust and privacy"

Work Completed

ECMA Std 205 / E-COFC V2.0 (Extended - Commercially Oriented Functionality Class)

ECMA TR78 / Common Criteria Protection Profile of the E-COFC/Public Business Class

ECMA


Laws
Data Security,
Signature, ...
PKI-Forum
CC
Common Criteria
TCPA
Trusted Computing
Platform Alliance
ISO 9000, CMM,
SPICE, ...
Sec.-Products /-
Protocols
SET, HBCI, ...
E -
Business
BSI 7799,
GMITS, et al.
Audit, Assessment
Related Defacto
Standards
RossettaNet, ORB, ...
Java...
Internal Regulations
Basic International Standards
ISO, W3C ...
SGML, XML, SOAP, UDDI, XSL ...
Security-Techniques
Encryption, ... Time stamps
- also ISO-Standards

ECMA

Issues addressed

- General problems of standards
- Problems of e-business
- Why are CC and ISO17799 not enough?
- Approach of ECMA
- How it compares

ECMA

Problems of Standards

often

- too slow (e.g. ISO OSI 7 levels)
- not cost-effective to use (e.g. ISO 9000)
- too complex (e.g. Common Criteria)

therefore we see

- de facto Standards (e.g. TCP IP, Linux)
- proprietary dominance (e.g. Microsoft)
- restricted compatibility (e.g. UNIX, Java)

but there are also

- success stories, e.g. SGML, XML

Problems of E-Business (1)

Level 0 *(mostly unknown theory)*

- Numbers, Complexity, Algorithms

Level 1 *(widely known building blocks)*

- Encryption (a/symmetric, public /privat. keys)
- MAC (message authentication code)
- Signature (used internally for MACs)
- Certificate (e.g. for public keys of a person)
- Certification Authority
- CRL (certificate revocation list)

Level 2 *(famous protocols)*

- SET, HBCI, ...

ECMA

Problems of E-Business (2)

Level 3 (Applications on top of those protocols)

not below: cooperation of mechanisms as Authentication, Access Control, Audit Trail, Generation, Initialization, Administration

Who can estimate security risks?

Problems of Operation + Administration + Environment
Holes often “border problems“ as generation of keys, personalization, life time of certificates

essential risks only within the application

manifold protocols and Applications

ECMA

Problems of E-Business (3)

Variety of applications

e.g. life time of certificates (CRL-Mgt.!)

a. Stock Trading (*life time of days*)

b. Buying houses (*life time of tens of years*)

ECMA

Secure system basis by Evaluation according CC

- Functional Criteria (Security functionality: from access control to pseudonymity)
- Assurance Criteria (EAL: Levels 1- 7)
- Security Targets (Threats, usage environment, objectives: Funct. Crit. + EAL)
- Protection Profiles (basis for comparisons)

Formal scheme for evaluations by independent experts

ECMA

Can CC be the answer?

+ CC-Evaluations: internationally accepted
+ (almost) all functions are addressed

<u>but</u>

- (broadly accepted) PPs are (still) missing
- “evaluated as presented“ problematic for SW
- trust gap: evaluation authority vs. plausibility
- expensive without direct advantage for user

ECMA Can ISO17799 be the answer?

BSI 7799 Part 1 via Fast Track now ISO 17799

compendium of measures by the operator of IT

comparable to

- the German „Grundschutzhandbuch“
- ISF “Standard of Good Practice“

all successfully used by many organisations

but

can we trust buraucratic controls alone?

And Industry is afraid of something like ISO 9000

ECMA

Unresolved issues

Customers and/or Business Partners

- trust without „understanding“
- no contribution to assess risks
- no advice for actions to be taken in case of incidents
  - evidence to be provided
  - how to proceed
  - conflicts to be expected

“High-Level Understanding“ also crucial für designers, implementors etc.

ECMA TC36 IT-Security

E - COFC: Extended Commercially Oriented Functional Criteria

Enterprise Business Class

Single potentially distributed Enterprise / CompanyUsers sign company contract /
One legal party, the company

Contract Business Class

Set of companies/Defined methods of operation / Legally governed by contract /
+ ”Regulatory Board”

Public Business Class

Provider-Customer relationship / Pre-existing contracts / Governed by Consumer Law
+ International laws and jurisdictions

Preparations for an: Open Business Class

ECMA Central Concept: Business Actions

May consist of arbitrary interactions between partners

- e.g. advertisement + order

Partners have distinguished roles

- which have to be taken into account wrt security

Several partners may be involved

- independent of specific protocols/mechanisms

ECMA

Benefits

Mapping from real applications to E-COFC possible because of general nature of interactions

E-COFC complete with respect to security issues

E-COFC supports design + evaluation of products via the E-COFC-PP with help for mapping

- *Objectives*,
- *Threats*,
- *Measures*, ...

on to CC building blocks!

ECMA

Comparison: RossettaNet

Goal of RossettaNet: uniform data formats thanks to XML for standardized types of „Business Actions“:
Query, 1-Step-Order, Status query

“Security“ restricted to the use of 3 mechanisms:
Secure channel, Signature, Time stamps within data structures

Sound Basis for restricting unnecessary variety
but security is only estabished bottom-up

ECMA

Approach and Levels

Public Business Class

Levels of *Threats*/ of *Deceit*/ of *Counter Measures*:

6. Business (contracts) <= E -COFC!
5. Pragmatic (context) <= Security Targets
4. Semantic (content) <= CC
3. Syntactic (language) <= RossettaNet
2. Implementation (signals and codes) <= Correctness
1. Physical (wires and devices) <= Correctness

ECMA

Intended Usage

Guidance for understanding measures against threats

- some plausibily for the operator (what to do)
- some plausibility for the user (whom to trust)
- in case of bottom-up correctness proofs
- in case of designing protocols and applications

Help for CC evaluations

Help for Security Target writing

Help for Protection Profile writing

E-COFC usable as framework or reference model

?

Questions?