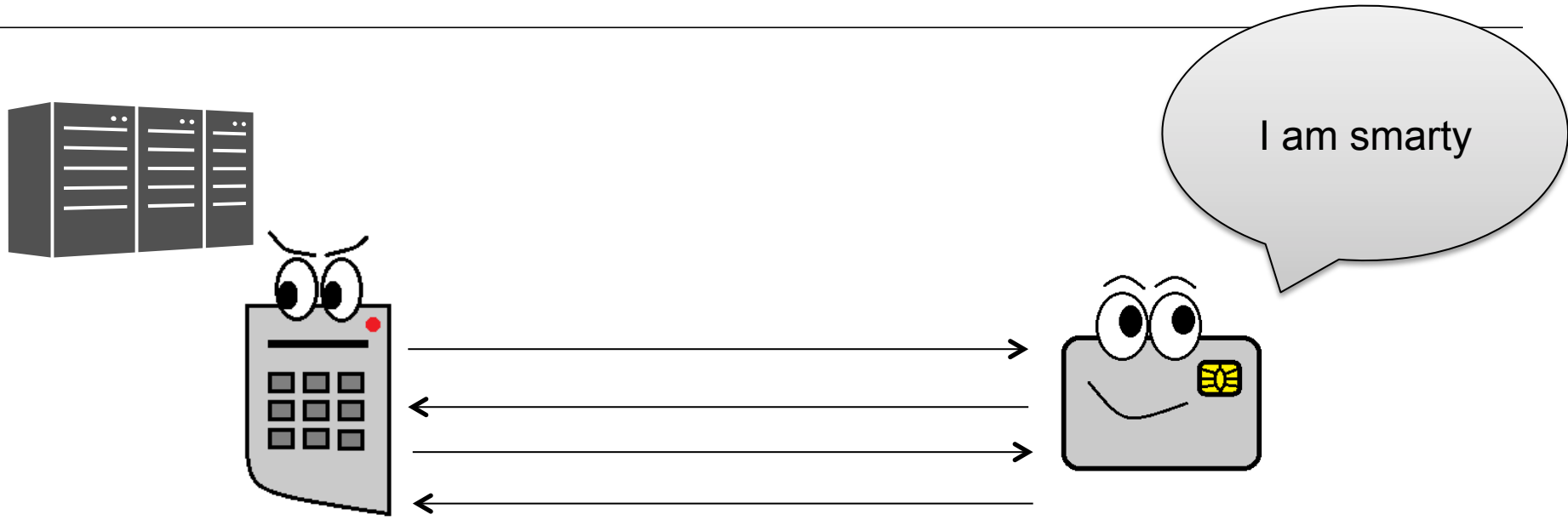
The ISO Standardization Process of PLAID: A Cryptographer's Perspective

Real World Cryptography Workshop 2015

Arno Mittelbach

based on joint work with Jean Paul Degabriele, Victoria Fehr, Marc Fischlin, Tommaso Gagliardoni, Felix Günther, Giorgia Azzurra Marson and Kenneth G. Paterson

PLAID: Protocol for Lightweight Authentication of Identity



Access granted/denied

PLAID is a general purpose smart card authentication protocol.

ISO standardization of PLAID

PLAID → Standardized by ISO → **World-class Authentication Protocol**

> International Standards make things work. They give world-class specifications for products, services and systems, to ensure quality, safety and efficiency.
>
> [ISO webpage]

This Talk

- PLAID is not a world-class authentication protocol
- (If PLAID is an indicator, then) the standardization process does not seem to work for cryptographic standards.

The history of PLAID

2006

Australian
Department
of Human Services

PLAID

ROYAL HOLLOWAY UNIVERSITY OF LONDON

+

TECHNISCHE UNIVERSITÄT DARMSTADT

2014

to SSR'14

ISO/IEC 25185-1

Australian Department of Human Services

PLAID

„Fast Track“

AS-5185-2010

TECHNISCHE UNIVERSITÄT DARMSTADT

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

Understanding PLAID

Break Cards

Active/Passive

Key Secrecy

Leakage

„Authentication Security“

Forward Secrecy

Break Terminals

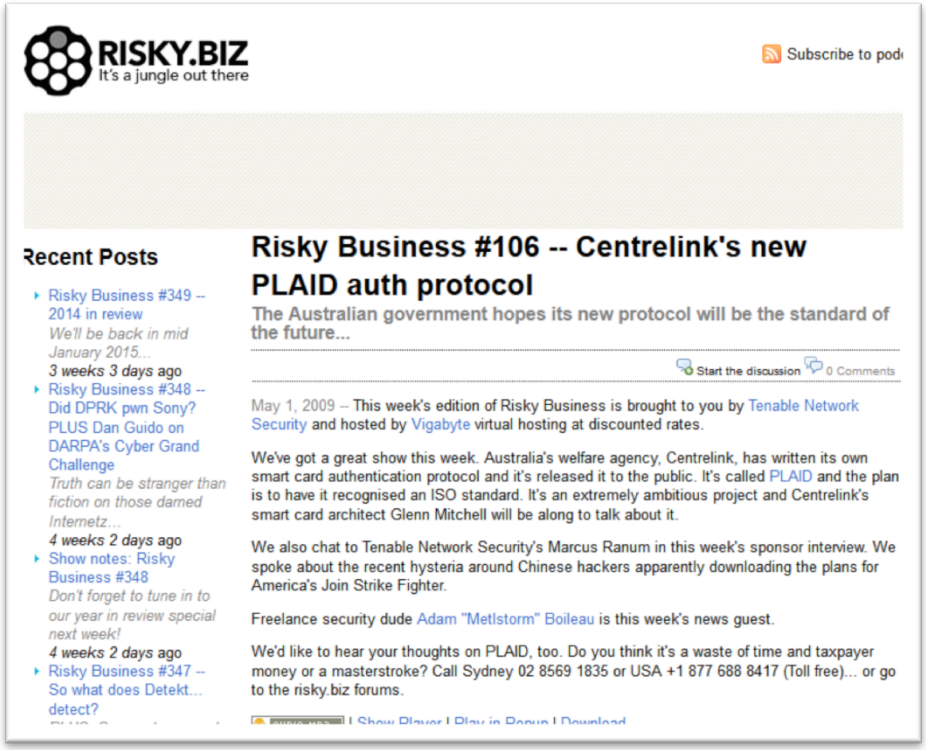
Protocol Goals

Identity Hiding

Privacy Aspects

Untraceability

Interview with Centrelink‘s smart card architect


RISKY.BIZ
It's a jungle out there

Subscribe to pod

Recent Posts

- Risky Business #349 -- 2014 in review
  We'll be back in mid January 2015...
  3 weeks 3 days ago
- Risky Business #348 -- Did DPRK pwn Sony? PLUS Dan Guido on DARPA's Cyber Grand Challenge
  Truth can be stranger than fiction on those darned Internetz...
  4 weeks 2 days ago
- Show notes: Risky Business #348
  Don't forget to tune in to our year in review special next week!
  4 weeks 2 days ago
- Risky Business #347 -- So what does Detekt... detect?

Risky Business #106 -- Centrelink's new PLAID auth protocol

The Australian government hopes its new protocol will be the standard of the future...

Start the discussion 0 Comments

May 1, 2009 -- This week's edition of Risky Business is brought to you by Tenable Network Security and hosted by Vigabyte virtual hosting at discounted rates.

We've got a great show this week. Australia's welfare agency, Centrelink, has written its own smart card authentication protocol and it's released it to the public. It's called PLAID and the plan is to have it recognised an ISO standard. It's an extremely ambitious project and Centrelink's smart card architect Glenn Mitchell will be along to talk about it.

We also chat to Tenable Network Security's Marcus Ranum in this week's sponsor interview. We spoke about the recent hysteria around Chinese hackers apparently downloading the plans for America's Join Strike Fighter.

Freelance security dude Adam "Metlstorm" Boileau is this week's news guest.

We'd like to hear your thoughts on PLAID, too. Do you think it's a waste of time and taxpayer money or a masterstroke? Call Sydney 02 8569 1835 or USA +1 877 688 8417 (Toll free)... or go to the risky.biz forums.

| Show Player | Play in Popup | Download

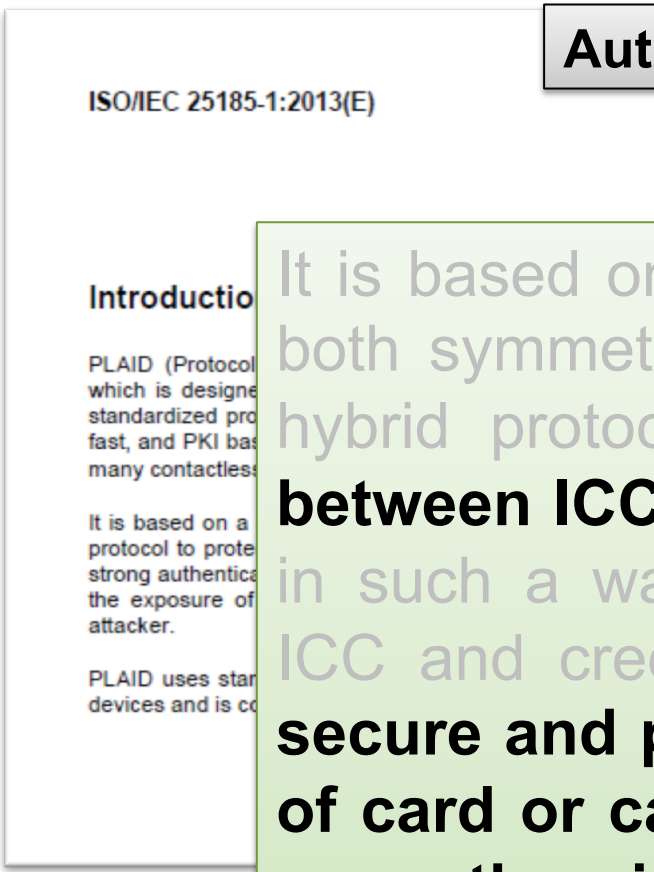
Identity Hiding

Untraceability

„PLAID was designed in order to ensure that all the air traffic is sufficiently scrambled so that **there is no way to identify the card involved in the transaction and therefore the person**.“

What PLAID aims for according to the ISO draft

Authentication Protocoll for smart cards


ISO/IEC 25185-1:2013(E)

Introductio

PLAID (Protocol
which is designe
standardized pro
fast, and PKI bas
many contactless

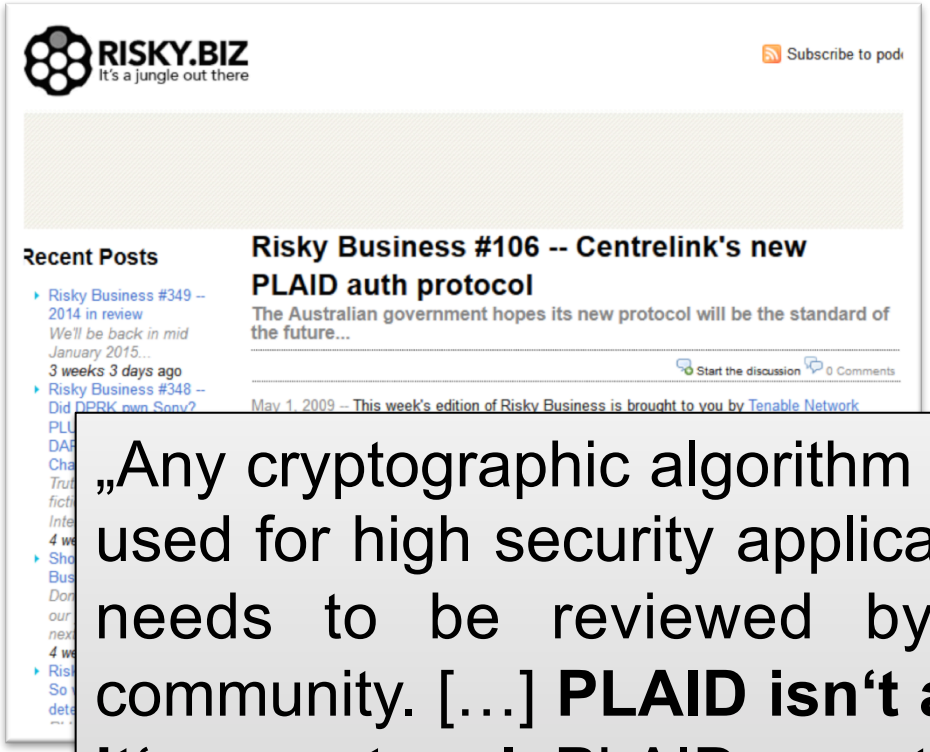
It is based on a
protocol to prote
strong authentica
the exposure of
attacker.

PLAID uses star
devices and is co

It is based on a cryptographic method, which uses both symmetric and asymmetric cryptography in a hybrid protocol to **protect the communications between ICCs and terminal devices**. This is done in such a way that **strong authentication** of the ICC and credentials is possible in a **fast, highly secure and private** fashion **without the exposure of card or cardholder identifying information or any other information which is useful to an attacker.**

Related Work?

Interview with Centrelink‘s smart card architect



„Any cryptographic algorithm [...] which is supposed to be used for high security applications needs to be open and needs to be reviewed by the wider cryptographic community. […] **PLAID isn‘t a cryptographic algorithm, it‘s a protocol**. PLAID uses two cryptographic algorithms [RSA and AES]. […] So, the actual cryptographic exchange […] is based on two well established, well reviewed and considered secure algorithms.“

ROYAL HOLLOWAY UNIVERSITY OF LONDON

TECHNISCHE UNIVERSITÄT DARMSTADT

Unpicking PLAID

A Cryptographic Analysis of an ISO-standards-track Authentication Protocol

Jean Paul Degabriele[1] Victoria Fehr[2] Marc Fischlin[2] Tommaso Gagliardoni[2]
Felix Günther[2] Giorgia Azzurra Marson[2] Arno Mittelbach[2] Kenneth G. Paterson[1]

[1] Information Security Group, Royal Holloway, University of London
[2] Cryptoplexity, Technische Universität Darmstadt, Germany
{j.p.degabriele,kenny.paterson}@rhul.ac.uk, marc.fischlin@cryptoplexity.de,
{victoria.fehr,tommaso.gagliardoni,giorgia.marson,arno.mittelbach}@cased.de,
guenther@cs.tu-darmstadt.de

Abstract. The Protocol for Lightweight Authentication of Identity (PLAID) aims at secure and private authentication between a smart card and a terminal. Originally developed by a unit of the Australian Department of Human Services for physical and logical access control, PLAID has now been standardized as an Australian standard AS-5185-2010 and is currently in the fast track standardization process for ISO/IEC 25185-1.2. We present a cryptographic evaluation of PLAID. As well as reporting a number of undesirable cryptographic features of the protocol, we show that the privacy properties of PLAID are significantly weaker than claimed: using a variety of techniques we can fingerprint and then later identify cards. These techniques involve a novel application of standard statistical and data analysis techniques in cryptography. We also discuss countermeasures to our attacks.

Keywords. Protocol analysis, ISO standard, PLAID, authentication protocol, privacy

1

Summary

cryptographic evaluation:

- weak privacy,
- uncommon design strategies,
- not recommended

TECHNISCHE UNIVERSITÄT DARMSTADT

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

It is based on a cryptographic method, which uses both symmetric and asymmetric cryptography in a hybrid protocol to protect the communications between ICCs and terminal devices. This is done in such a way that strong authentication of the ICC and credentials is possible in a fast, highly secure and private fashion **without the exposure of card or cardholder identifying information or any other information which is useful to an attacker.**

General Concerns

not authenticated!
→ Key Legacy Attack
→ Key Revocation?

TECHNISCHE UNIVERSITÄT DARMSTADT

non-standard use of PKE

(KeySetIDs)

PKCS#1.5 Padding used

ICC

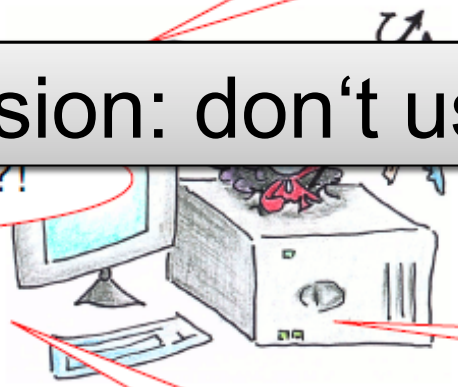
index	RSA	AES
2	pk_2	K^{ID}
7	pk_7	
*	pk^*	K^*

IFD

	RSA	AES
	sk_7	K_7
34	sk_{34}	K_{34}

Conclusion: don't use PLAID

trial-decryptions?!



AES

sion)

sending payload to the card

CBC-mode with IV= 0^n

no forwa ecrecy!

$AES_{k_{sess}}$

static entity authentication

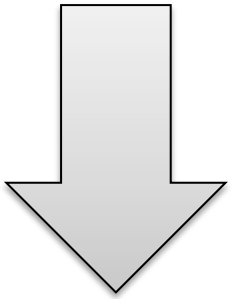
reusing session key

non-standard Padding

secured with $k_{session}$ (optio

The ISO Standardization Process of PLAID

PLAID



ISO/IEC JTC 1/SC 27 WG 2
Cryptography and security mechanisms

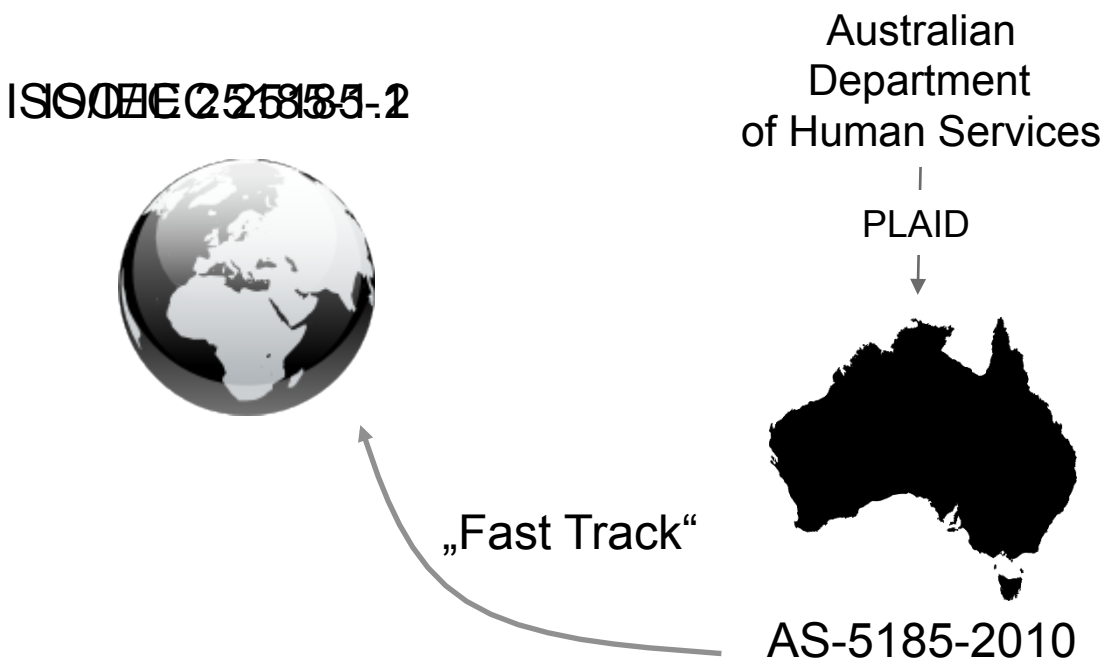
ISO/IEC JTC 1/SC 17 WG 4
Integrated circuit card with contacts

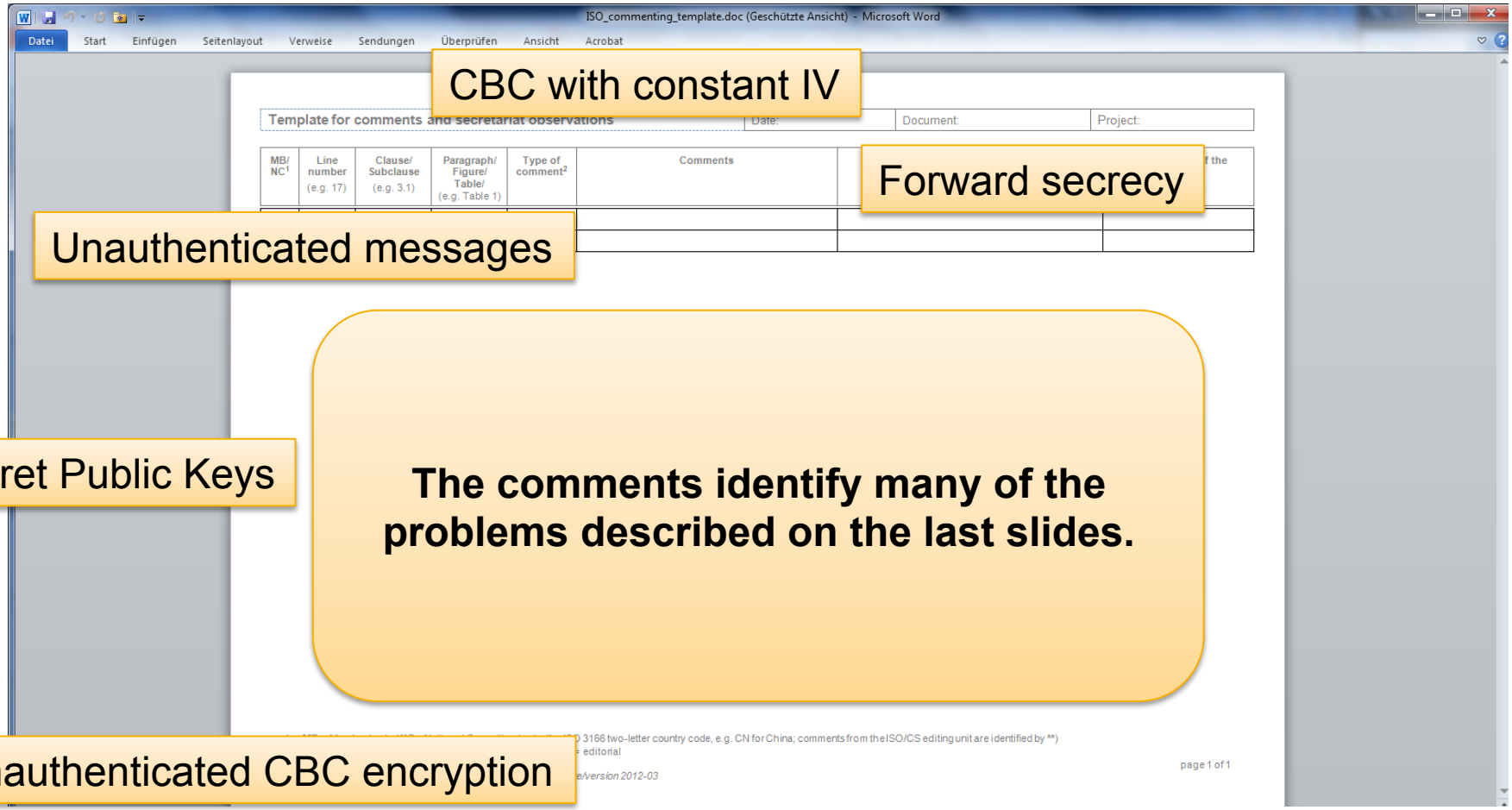
„I would not be surprised if PLAID was introduced into SC 17 on purpose in order to circumvent a more thorough scrutiny.“

[meeting of NIA-01-17-04]

The ISO Standardization Process of PLAID

2014





CBC with constant IV

Forward secrecy

Unauthenticated messages

Secret Public Keys

The comments identify many of the problems described on the last slides.

Unauthenticated CBC encryption

PKCS#1.5 RSA Padding

Editor‘s response to comments

First message is unauthenticated

That is an implementation issue.

CBC does not provide data integrity

[The last blocks are verified by the ICC] and since CBC validates every bit of preceding data, any modification would be detected by the ICC..

DE36 on secret public RSA keys

Template for comments and secretariat observations — Date: 2013-09-15

MB/ NC[1]	Line number (e.g. 17)	Clause/ Subclause (e.g. 3.1)	Paragraph/ Figure/ Table/ (e.g. Table 1)	Type of comment[2]	Comments	Proposed change	Project Editor Proposed Action and/or comment resolution
DE29	8	Table 2	ed	In the case of RSA keys longer than or equal to 256 bytes (state of the art RSA key lengths) extended length and / or command chaining is required for the response data field of the Initial Authenticate command and the command data field of the Final Authenticate command. The draft specifies by means of the CLA byte in table 2 that the support of extended length is mandatory in this case, so that only one command / response APDU is required to transport the data.	Add a statement e.g. as follows: If RSA keys with lengths longer than or equal to 256 bytes are supported, the support of extended length is mandatory, so that only one command / response APDU is required to transport the data.	Accept – but suggest everything after the second comma is unnecessary, and suggest adding APDU after word "length"
					v1.5-padding. This is problematic in several ways: – To the best of our knowledge there are no cryptographic results which actually guarantee that the public key cannot be		not aware of any publicly available information which guarantees that the public key cannot be recovered from ciphertexts. However, this concern hasn't stopped

1 MB = Member body / NC = National Committee (enter the ISO 3166 two-letter country code, e.g. CN for China; comments from the ISO/CS editing unit are identified by **)
2 Type of comment: ge = general te = technical ed = editorial

ISO/IEC/CEN/CENELEC electronic balloting commenting template/version 2012-03

Comment: To the best of our knowledge there are no cryptographic results which actually guarantee that the public key cannot be recovered from ciphertexts.

Date: 2013-09-15 | Document: ISO/IEC DIS 25185-1 | Project:

Proposed change	Project Editor Proposed Action and/or comment resolution
m ciphertexts. – Protecting the public key not only amounts to secure storage of the key, but also concerns side-channel free computations with the key. For RSA, there are no established mechanisms to protect public key operations against side channel analysis, leading to huge effort for the COS vendor. This is	the usage of RSA in the vast majority of all PKI systems (including SSL/TLS). – Second point - Smartcards are typically evaluated under Common Criterion Protection Profiles and/or other

ISO/IEC/CEN/CENELEC electronic balloting commenting template/version 2012-03

Response: we are also not aware of any publicly available information which guarantees that the public key cannot be recovered from ciphertexts. **However, this concern hasn't stopped the usage of RSA in the vast majority of all PKI systems (including SSL/TLS).**

DE01 on unclear security properties

Template for comments and secretariat obse

MB/ NC[1]	Line number	Clause/ Subclause	Paragraph/ Figure/	Type of comment[2]	Comments	Proposed change	Project Editor Proposed Action and/or comment resolution
							Discuss The protocol is designed primarily to replace existing (very weak and regularly broken) protocols used in Physical Access Control Systems (PACS) and/or some related LACS where speed is of the essence. It has been arranged for Glenn Mitchell to attend and will discuss the practicality of cryptographic proofs in ISO documents given that RSA and other ciphers cannot be formally proved. Not clear what changes are recommended by DE
DE02				ge			

1 MB = Member body / NC = National Committee (enter the
2 Type of comment: ge = general te = technical

ISO/IEC/CEN/CENELEC electronic balloting commenting ter

Comment: The security properties of the protocol and the requirements on the chosen primitives seem to be unclear. […] **To make the security properties clear, it is recommended to draw up a cryptographic security proof.**

Response: will discuss the practicality of cryptographic proofs in ISO documents given that RSA and other ciphers cannot be formally proved.

Not clear what changes are recommended by DE to the document as a result of this comment.

These were all comments for DIS 1

Conclusion

- Be careful with PLAID
- PLAID and especially the current DIS does not live up to ISO‘s expectations (or ours)

> International Standards make things work. They give world-class specifications for products, services and systems, to ensure quality, safety and efficiency.
>
> [ISO webpage]

- (If PLAID is an indicator, then) the standardization process does not seem to work for cryptographic standards.

Thank You

Arno Mittelbach
TU Darmstadt
Mornewegstr. 30
64293 Darmstadt

arno.mittelbach@cased.de
www.arno-mittelbach.de

P.S. Arno plans on finishing his Ph.D. in the next six months and interesting job offers in the Darmstadt area are always welcome.