

MullPon

Dossiernummer KvK Friesland: 01083315; Algemene Voorwaarden voor Dienstverlening gedeponeerd aldaar (nr. 3326)

Lynbaen 9

8563 AZ Wijckel (F); The Netherlands

Tel: +31-(0)514-605 942; Fax: +31-(0)514-605 945; GSM: +31-(0)641 267 617

E-mail: pietpont@mullpon.com

Confidential / Vertrouwelijk zoals bedoeld in Artikel 7 van onze levervoorwaarden

In deze versie is per deel aangegeven tussen [] of de informatie mag worden vrijgegeven in het kader van de WOB of niet, en zoniet waarom niet; daarbij worden de volgende coderingen gebruikt:

[WOB-vrij] dit deel mag worden vrijgegeven in het kader van de WOB

[WOB confidential 10c] dit deel mag NIET worden vrijgegeven, omdat dat bedrijfs- en fabricage gegevens betreft, die vertrouwelijk aan de overheid zijn meegedeeld

[WOB confidential 10b] dit deel mag NIET worden vrijgegeven, omdat dat de veiligheid van de staat zou schaden, in dit geval met name wegenskans op doorbreking van het kiesgeheim

RIES-2008

CRYPTO

Cryptographic architecture for RIES-2008 and RIES-KOA

by

Pieter G. Maclaine Pont

Wijckel, July 12, 2006

Version 0.95WV DRAFT – met markering vertrouwelijkheid ivm WOB
en verwijdering van de vertrouwelijke delen

Informatie in dit document is uitsluitend toegankelijk voor personen, die daartoe een “non-disclosure” overeenkomst met het hoogheemraadschap van Rijnland en MullPon vof zijn aangeaan

Betr.: volgens onze offerte van 30 augustus 2005 voor S. Bouwman / Het Waterschapshuis

Table of Contents *[WOB-vrij]*

Table of Contents..... 2

Literature references 3

1994 Januari 11 3

Significant changes and remarks 5

- Version 0.1 to version 0.2..... 5
- Version 0.2 to version 0.3..... 5
- Version 0.3 to version 0.8..... 5
- Version 0.8 to version 0.9..... 5
- Cryptographic architecture for RIES-2008 and RIES-KOA 7

Introduction 7

The reader for who this document is mend..... 7

Cryptography and RIES-KOA 8

- Problem definition 8
- The base of the RIES-KOA solution 8

The cryptographic support for different components of RIES-KOA 10

- The off-line components Prepare and Tally..... 10
 - Salt_part_gen utility..... 10
 - Key handling by Prepare and Tally 11
 - Cryptographic Integrity Assurance by duality 11
- The on-line component Voting_Window 11
 - PCF-like design 12
 - TPCF set-up and instruction set..... 12
 - TPCF-util functions 13
 - Salt_part_gen 13
 - Set Master Key (SMK) 13
 - TPCF-GenKey 14

Recommendations..... 16

Conclusions 16

Literature references [WOB-vrij]

[Meyer] Cryptography, a new dimension in computer data security; Carl H. Meyer, Stephen M. Matyas; John Wiley & Sons, 1982; ISBN 0-471-04892-5

[Robers]RIES: Rijnland Internet Election System > RIES: Fully transparent election system > Downloads, Herman Robers, November 1998

[CCA] Common Cryptographic Architecture - Cryptographic Application Programming Interface; D. B. Johnson, G. M. Dolan, M. J. Kelly, A. V. Le, S. M. Matyas; **IBM SYSTEMS JOURNAL**, VOL 30, NO 2, 1991

[FIPS140-1] FIPS PUB 140-1; *SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES*; U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY; 1994 Januari 11

[IBMPFC] IBM PROGRAMMED CRYPTOGRAPHIC FACILITY (GI11-1380-00); 5740-XY5, Programmed Cryptographic Facility 1.1, is replaced by Integrated Cryptographic Service Facility, available as part of 5694-A01, z/OS Version 1, announced in Software Announcement [204-017](#), dated February 10, 2004, or 5655-G52, z/OS.e Version 1, announced in Software Announcement [204-016](#), dated February 10, 2004.

[IBM 4758] IBM 4758 PCI Cryptographic Coprocessor; CCA Basic Services Reference and Guide - Release 2.54 - IBM iSeries PCICC Feature; IBM Corporation; Thirteenth Edition (December, 2004)

[PKCS5] PKCS #5 v2.0: Password-Based Cryptography Standard; RSA Data Security, Inc. Public-Key Cryptography Standards (PKCS); RSA Laboratories March 25, 1999

[RIES-2004] www.rijnland.net/ries

[RIES-2004 general project description] RIES: Rijnland Internet Election System > RIES: Fully transparent election system > RIES for two formal elections serving more than 2,2 million voters in 2004, *RIES* (Rijnland Internet Election System) for two formal elections serving more than 2,2 million voters in 2004, March 2nd 2005, version 1.31



[RIES-2004 facts and figures] RIES: Rijnland Internet Election System > RIES: Fully transparent election system > RIES Facts and Figures, *RIES* facts and features sheet, March 2nd 2005, version 1.3

[NL Octrooi 1023861] <http://www.octrooicentrum.nl>; look for patent 1023861 [M1]

[Overeenkomst tot regeling van mede-eigendom] <http://www.octrooicentrum.nl>; octrooi 1023861, zie gepubliceerde overeenkomst tussen P.G. Maclaine Pont en Hoogheemraadschap van Rijnland[M2]

[Abel] RIES-2008 Abel; vertrouwelijk document dat diverse implementatie aspecten van Abel beschrijft; P.G.Maclaine Pont; v 0.8 december 2005

[Abbrev] RIES abbreviations and definitions; samenvatting van de diverse gebruikte afkortingen, begrippen, definities en formulas van RIES; P.G.Maclaine Pont; v 4.1 januari 2006

[CoE STD] Legal, operational and technical standard  e-voting, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum; Council of Europe publishing, April 2005; ISBN 92-871-5635-2 

[Hubbers] <http://www.cs.kun.nl/ita/publications/papers/hubbers/compsac2005.pdf> ;

RIES – Internet Voting in Action, Engelbert Hubbers; Bart Jacobs and Wolter Pieters; Institute for Computing and Information Sciences; Radboud University Nijmegen; PO Box 9010, 6500 GL Nijmegen; E.Hubbers,B.Jacobs,W.Pietersg@cs.ru.nl

[Pieters] <http://www.cs.ru.nl/W.Pieters/ACMforum.pdf>; Internet voting *not* impossible; Wolter Pieters (Nijmegen, Netherlands), Joe Kiniry (Dublin, Ireland);
November 16, 2004

Significant changes and remarks [WOB-vrij]

Version 0.1 to version 0.2

- Entire document:
 - Restricted circulation to personnel under non-disclosure agreement, on need-to-know basis only.
 - Updates in new versions viable only in the printed version.
- First step to formal documentation.

Version 0.2 to version 0.3

- New design for key generation
- Separation of control of secret keys over different parties
- Description of key management architecture in short notation and bullets

Version 0.3 to version 0.8

- Full texts on architecture
- Clean-up version
- First level, suitable for limited outside discussions and reviews.

Version 0.8 to version 0.9

- Clear key input for EMK
- VALkm can be compared to last value of VALkm, stored on disk; only acceptance question to TTPI of NOT equal; in that case last and former-last VALkm are given to TTPI as well
- Validation of the TPCF functions
- Feedback from Arnout Hannink
- Final clean-up

Version 0.9 to version 0.95

- Improvement of text that describes the goal of the separation of key generation and handling between two parties
- Last salt_part entry by KOA *specialist* or TTPI
- Text on filtering salt_part_n (more than one space character removed)
- Several small text corrections

- **Cryptographic architecture for RIES-2008 and RIES-KOA**

Introduction [WOB-vrij]

In 2008 all Dutch water boards will organize one common, country-wide election event for all 12.000.000 Dutch inhabitants. All votes for these countrywide water board elections can be cast both by regular mail and the Internet. The technical developments to create the facilities for these elections are referred to as *RIES-2008*. RIES-2008 is a further development of the mail and Internet election system RIES, used in 2004 and 2005 for the 2.200.000 voters of the Rijnland and De Dommel water boards and referred to as [*RIES-2004*].

In addition, an Internet election for KOA (a department of the Dutch Home Office) is prepared, based on RIES-2004 that will be used by Dutch citizens living abroad to cast their votes through the Internet in the parliamentary elections to be held around November 2006. This version of RIES is referred to as *RIES-KOA*.

This specific document will handle the general cryptographic design principles, used in RIES-KOA and partly in RIES-2008.

The information in this document is an extension to patent [NL Octrooi 1023861] and might create a new patent application. According to the current agreement [Overeenkomst tot regeling van mede-eigendom] between the owners of [NL Octrooi 1023861], these owners share the ownership of all mechanisms and inventions described in this document. The ownership of all software and system designs, implementations and prototypes belongs to the same parties that created RIES-2004.

The reader for who this document is mend [WOB-vrij]

This document should give background to the reader of the cryptographic design and its base principles for RIES-KOA. It is written for readers with a general interest in RIES-KOA and for implementation and review purposes.

Due to the sensitive nature of cryptographic functions implemented in software only, this document cannot be made public.

Cryptography and RIES-KOA

Problem definition [WOB-vrij]

RIES, or better: the underlying mechanism DVSS is based on the deployment of a symmetrical algorithm [Robers]. In its functions, RIES/DVSS is based on functions that create an asymmetrical relationship between quantities. Some of the prime requirements of any voting system, like voter secrecy, even to insiders of RIES, are based on that. However, since the underlying algorithm is symmetrical (in RIES-2004 it is DES and 3DES), knowledge or availability of specific system keys to insiders (e.g. TTPI) will give them the opportunity to breach this requirement.

In its design this exposure could be overcome in a pragmatic way by making use of hardware cryptographic facilities [IBM4758], that meet applicable physical security standards (e.g. a tamper-responding hardware design certified under FIPS PUB 140-1 [FIPS140-1]) and the use of a cryptographic key design, like IBM's Common Cryptographic Architecture [CCA], that would remove this exposure and would introduce capabilities to auditors to validate that all cryptographic functions are used in the proper way [IBM 4753].

Due to budget and time restrictions, hardware cryptographic technology will not be used in case of RIES-KOA. In this version this document will only discuss the cryptographic design for RIES-KOA.

The base of the RIES-KOA solution [WOB-vrij]

For RIES-KOA, a software implementation has been designed, that does allow a separation of cryptographic functions in such a way, that the voting application programs themselves do not handle secret cryptographic keys. Instead, these applications refer to secret keys only in a logical way, using a specific architected set of cryptographic functions. All sensitive cryptographic operations are then processed by a separate piece of software, the so-called TTPI Cryptographic Facility (TPCF). TPCF is a simplified design of IBM's Programmed Cryptographic Facility [IBMPCF], based on the architecture for DES as described in [Meyer]. TPCF stores all cryptographic keys in a Cryptographic Key Data Set (CKDS) in a protected form, e.g. encrypted under a secret Master Key (KM). This KM is not installed on any storage of the server during regular, non-RIES functions of that server and only made available through a separate read-only device or file that is installed in the server only when required to run a voting application. Furthermore, the use of KM by TPCF requires the entry of a secret password (PW).

Although this design does not even come close to the use of [CCA] cryptographic hardware, it allows for some control on the abuse of cryptographic keys, if

- The software on the server that manages the keys [TPCF] is carefully reviewed on its functioning

- Integrity on the application base of the server can be guaranteed
- A full separation is enforced between personal that handle the read-only device or file, that contains KM in protected form and the password PW, needed to use KM
 - The access to the read-only device or file, that contains KM in protected form is well maintained and handled by a party, responsible for the technical operation of the server, containing the RIES-application (e.g. SURFnet operators)
 - The control on the use of KM, exclusively by the proper software (TPCF), is limited only to the insiders, responsible for RIES (e.g. TTPI), through their knowledge of PW.
 - Both parties cannot have knowledge of the actual value of KM, unless they would cooperate to achieve this knowledge.

The cryptographic support for different components of RIES-KOA

The off-line components Prepare and Tally [WOB-vrij]

For RIES-KOA both components are based on the RIES-2004 design. In Prepare and Tally several cryptographic functions, based on secret keys, are used. These include the following secret cryptographic keys:

- Kgenvoterkey, a 16 byte 3DES key-generation key
 - Kp, a 8 byte Personal Key, to be translated in an 34AN value, to be entered through the PC keyboard by a voter
-

[WOB-confidential 10c]

Salt_part_gen utility [WOB-confidential 10c] [WOB-confidential 10b]

Key handling by Prepare and Tally [WOB-confidential 10c] [WOB-confidential 10b]**Cryptographic Integrity Assurance by duality [WOB-vrij]**

To assure that no bit errors created randomly by the PC hardware will damage the results of Prepare and Tally, these applications will be performed on two separate off-line PC's. During the calculations a running hash total on all the generated values is calculated. At completion of the calculations, these hash totals from both PC's are compared: in case they are equal the outcome can be considered to be without (bit) errors.

The on-line component Voting_Window [WOB-vrij]

The Voting_Window application is the main server application, responsible to allow the voter to cast his vote. The use of cryptographic keys by the server application itself is limited to

- Kpbs_b, a 16 byte 3DES MAC generating key, that generates for each properly received vote on Ballot-Box Server b a Vote Receipt Confirmation (VotRecCon).

This VotRecCon is an 8 byte MAC value calculated over the combination of the Pseudo Identity of the Voter (VnPID) and his Virtual Ballot (VnC_x) he cast.

For RIES-KOA 2 (two) Voting_Window servers in two different locations will be used, referred to as BallotBox servers BBS_1 and BBS_2. On both BallotBox servers the same Kbbs_b will be used. This key will be referred to as Kbbs_0.

[WOB-confidential 10c] [WOB-confidential 10b]

-

In addition, SSL keys are used. But these are handled by a fully separated implementation and taken care of by the network group. In this document the SSL set-up will not be discussed.

PCF-like design [WOB-vrij]

As a first step to enable migration to hardware cryptography, a separation has been implemented between the application tasks that perform the data-calculations and generations and the actual cryptographic calculations and handling of clear cryptographic keys. This separation concept is based in principles, defined for the IBM Programmed Cryptographic Facility [IBMPCF]. It will make it possible to introduce a hardware cryptographic facility in a later stage, without major changes to the application itself.

[WOB-confidential 10c] [WOB-confidential 10b]

TPCF set-up and instruction set [WOB-confidential 10c] [WOB-confidential 10b]

TPCF-util functions [WOB-confidential 10c] [WOB-confidential 10b]

1.

Salt_part_gen [WOB-confidential 10c] [WOB-confidential 10b]

Set Master Key (SMK) [WOB-confidential 10c] [WOB-confidential 10b]

SMK on the BalBox servers *[WOB-confidential 10c] [WOB-confidential 10b]*

TPCF-GenKey *[WOB-confidential 10c] [WOB-confidential 10b]*

Recommendations [*WOB-vrij*]

- Validation of the proper functioning with special, stand-alone DES and 3DES utilities and tools to make KM available in clear for test purposes only
- Full validation through the regular vote control possibilities of RIES itself
- Code review on all cryptographic software implementations after they have been fully completed and tested and are ready for production.

Conclusions [*WOB-vrij*]

Although software cryptography does offer very limited possibilities to create a cryptographic key management that prevents abuse by human insiders (e.g. to prevent that a single person or party can obtain knowledge of secret cryptographic keys), the given design is at least a step forward in that direction. In combination with proper organization measures an acceptable balance for the control of risks can be obtained.