RIES facts and features sheet

July 28th 2010, version 2.0

General

RIES (for Rijnland Internet Election System) is a multiple technology election system, developed in 2003 and 2004 for the Water Board elections at Rijnland and De Dommel to serve approximately 2,.2 million voters. An adapted version RIES-KOA has been applied in 2006 to enable Dutch citizens living out of The Netherlands to cast there votes for the parliament elections

The current version combines postal mail and Internet election technologies. Future versions might include GSM, SMS and other digital network technologies, in addition to conventional voting machine and ballot box election systems.

Since 2008, both the RIES documentation and source code and the related patent are in the open domain.

RIES *consists of*

1. **The initial stage**, in which an initial process on an isolated, off-line server complex (RIPOCS), stored in a fault, calculates *individual voter secrets* (to be distributed to all individual voters as part of their individual *election package*) and a *Reference File*. The input to this initial process consists of the database of all entitled voters, all eligible candidates and several general parameters.

2. **The election stage**, in which each voter returns their vote either by postal mail as a ballot (paper) or by Internet in the form of a cryptographic *DES Virtual Ballot Form*.

3. **The tally** stage in which the final results are calculated and information is published to allow all voters and independent parties to recount and validate the results.

Main features

***RIES* has been developed in a pragmatic, cost conscious way, which leads to the following main qualifications:**

1. The *RIES* Internet election scheme is extremely simple, straightforward and open ended.

a. Over 99.9% of today's Internet users are able to vote through *RIES* without any changes to their Internet connection or phone dial-in, their home computer and its software.

b. Practical tests and the results of the four 2004, 2005 and 2006 Internet elections, used by over 140,000 Internet voters, have shown that over 99.9% of all voters can cast their votes through the *RIES* Internet voting screens without any difficulty.

c. In addition, more conventional postal mail voting and ballot box voting is offered through *RIES*, without any requirement for the voter to pre-register the way he will cast his vote.

d. To take part in an election, all entitled voters receive an individual *election package* beforehand, containing the voting secrets, needed to cast an individual vote through the Internet, postal mail or ballot box.

2. The *RIES* election scheme is sophisticated, despite its simplicity.

a. Before the election starts, a *Reference File*, calculated by *RIES*, is published. This *Reference File* will allow for several checks on the entire election system by independent outsiders and for specific controls by all voters right after the elections are completed.

   Despite its simplicity, *RIES* is based on a sophisticated scheme, in which none of the voter secrets leave the voter's PC browser and are never shared with any election server, nor stored in any form with any party, including the election authorities, during the election stage. Only at the initial stage sensitive information is present with parties, who are equipped to enable sensitive postal mailings. At the end of the initial stage, all sensitive information is either destroyed or kept in safe storage at a notary public.

b. Right after the election part, individual voters can verify that their vote is counted in the final outcome. The voter can do this without giving away any "proof-of-vote". Independent parties can validate the *RIES* election results.

c. *RIES* allows for the acceptance and processing of multiple voting entries from the same voter in the same election. In the tally part, these entries can be compared and an automated decision can be made about the voter's real intended choice without any breach to the required confidentiality of each vote. This creates the possibility for the voter to vote once more by Internet or postal mail in case of uncertainty that the system processed the first attempt correctly, for example in case of a major network disturbance.

d. *RIES* allows for the issuing of a *replacement election package* to a voter, who claims not to have received the original one by postal mail (which will be rendered invalid). To prevent abuse, individual voters and independent parties can validate such changes afterwards.

e. *RIES-2008* allows for the validation that an election package can only be used to cast a valid vote by the voter the package is intended for; this is the so-called *Abel* (for *Abuse Elimination*) feature of RIES.

f. RIES election results are end-to-end auditable by any interested party (and have actually been audited by people from Radboud University).

g. Since 2006 additional modules have been added to RIES to assist in the preparation stage of elections. These administrative processes are based on pragmatic and effective network functions, to be used on different levels in the preparing organizations. These modules are open-source as well.

3. The technology required for running *RIES* is simple, straightforward and therefore reliable and low-cost.

a. The *RIES* Internet voting approach is mainly a store-and-forward system. That makes the system, its network and election servers simple and rugged to cope with the harsh Internet environment. During the election process, there is no need for a stateful conversation between the voter's home computer and a central election server, making the implementation of server and network redundancy extremely simple.

b. Network and server support requirements for a large-scale deployment of *RIES* are simple and straightforward. For the large-scale *RIES* elections in The Netherlands in 2004, 2005 and 2006 (in which 140,000 Internet voters took part) two sets of simple Intel architecture-based FreeBSD servers, with SSL offloading capabilities, have been used on different, isolated locations, offering an overcapacity of more then 97% during the largest peaks.

c. In addition, proper measures have to be taken against typical network risks, including the loose of an entire server location and spoofing and DDOS attacks. At the deployment of RIES in 2006 to 2008 that was designed and performed by SURFnet (www.surfnet.nl) through two server-complexes in different protected locations on distinctly different network paths, and internal defenses against spoofing and the detection of DDOS attacks.

d. Furthermore, the entire development of *RIES* took place on a budget, which was only a fraction of that of comparable development efforts, most of them leading to less sophisticated systems than *RIES*.

4. RIES principles and constructions are public.

- The *RIES* design is based on a sound concept; its election method is fully published.
- *RIES* is fully based on open-source coding. All RIES documentation is public and all RIES modules are open-source as well. See www.openries.nl for details (partially in Dutch).
- With the published design of *RIES* and the published election information only, any independent party can validate the *RIES* election counting and results. This was done for all *RIES* elections in 2004 through 2006 (by Radboud University).
- The construction of RIES is based on *DES Virtual Ballot System* (*DVBS*), for which international patent applications have been filed. These patents are available at no costs to any interested party in the deployment or further development of RIES open-source.
- In general, *RIES* meets all requirements that should be met by any network oriented election system suitable for formal (government) postal election processes.

Independent, reputable professional parties have extensively reviewed RIES

In spite of the low development costs, independent, reputable professional parties have extensively reviewed *RIES*. These include for the 2004-2006 timeframe:

- TNO, Delft (for an initial feasibility survey)
- A team of Peter Landrock's Cryptomathic, Aarhus Denmark (the cryptographic design)
- TNO Human Factors, Soesterberg (human factor aspects of the voter screens)
- Madison Gurka, Eindhoven (crystal-box security evaluation of server and network design)
- Bart Jacobs' external penetration team of Radboud University Nijmegen (external network and server penetration tests and independent election outcome validation)
- Burger@overheid, ICTU, Den Haag (large-scale end-user validation)
- Extensive specialist auditing has been done by the Dutch Home office for the 2006 parliament elections.

See http://www.openries.nl/downloads/external_reviews and http://www.openries.nl/ for lists of more recent reviews (partially in Dutch).

General election data of the 2004 through 2006 elections

Organized by:	**WB Rijnland/ Leiden**	**WB De Dommel/ Boxtel**	**Home Office**
Website:	**www.rijnland.net**	**www.dommel.nl**	
Total number of eligible voters:	**1,363,787**	**878,118**	**21.593**
Total number of seats:	**36**	**35**	**Parliament elections**
Total number of candidates:	**183**	**115**	**for non-inhabitants**
Total number of votes received:			
By postal mail:	**160,647**	**120,201**	**not applicable**
By Internet:	**72,235**	**50,196**	**19.929**

(Other water boards organized postal mail elections in the same timeframe and had a comparable turnout).
(Information about the Home Office project can be obtained through www.kiezenuithetbuitenland.nl).

In all elections, the *RIES* system lived up to all expectations. The system performed with a negligible number of complaints by voters and has been flawless in processing all postal mail and Internet votes. Solely based on the published working principles and election files, independent parties have been able to fully validate the results of the (Internet) elections.

The two water boards expressed their positive appreciation of this new election system and do regard the technology now as fully operational. In April 2005, Rijnland did apply *RIES* once more for a re-election in the Amsterdam district. All 26 Dutch water boards have prepared a countrywide combined election for November 2008 for all 12.300.000 adult citizens of The Netherlands with RIES, offering both Postal and Internet voting. For political reasons, only the Postal elections have been conducted (RIES was used for the processing).

RIES links and references

- **The two Dutch water boards, that did deploy *RIES* in 2004, are**
  - **The Rijnland District Water Control Board**
    - **Mail address:**
      - Hoogheemraadschap van Rijnland
      - Attn. Drs. Simon Bouwman / *RIES* project manager
      - c/o Het Waterschapshuis, PO Box 2180
      - 3800 CD Amersfoort
      - The Netherlands
    - Internet: www.waterschapshuis.nl
    - Telephone: +31 (0)33 460 3100
    - E-mail: s.bouwman@waterschapshuis.nl
  - **De Dommel Water Board**
    - **Mail address:**
      - Waterschap De Dommel
      - Attn. Mr. A.P.J. van Leengoed / Election project manager
      - PO Box 10001
      - 5280 DA Boxtel
      - The Netherlands
    - Internet: www.dommel.nl
    - Telephone: +31 (0)411 618 618
    - E-mail: avleengoed@dommel.nl

- **Literature References**
  - *RIES* related
    - [Robers] DES Smartcards in electronic elections, Herman Robers, November 1998
    - [Design] Design Information about *RIES*, the Internet Election System to be used by the Water Board Rijnland, Pieter G. Maclaine Pont, April 4th 2004
    - [Abbreviations] RIES Abbreviations and definitions v 1.2, P.G. Maclaine Pont, April 2004, special RIES project document
    - [Patent] Dutch patent application is pending under request **102 3861** since July 8th 2003
    - [Hubbers AG] Stemmen via internet geen probleem , (Internet voting, no problem) Engelbert Hubbers, Bart Jacobs, Automatisering Gids #42, October 15, 2004, p.15 (Dutch language)
    - [Hubbers RU] RIES - Internet Voting in Action, Engelbert Hubbers, Bart Jacobs and Wolter Pieters; Security of Systems, Nijmegen Institute for Computing and Information Sciences, Radboud University Nijmegen
    - See http://www.openries.nl/downloads/documentatie and http://www.openries.nl/ for more publications (partially in Dutch)
  - Interdisciplinary graduating student teams, managed by Piet Maclaine Pont, that proceeded the development of *RIES*
    - [ISCIT] on request from pietpont@mullpon.com
    - [wISCIT] on request from pietpont@mullpon.com
- **More information**
  - *RIES* has been developed by a team of small individual companies, cooperating as *TTPI* see www.ttpi.nl). These companies include
    - *MullPon*, owned and operated by Piet Maclaine Pont
    - *Magic Choice*, owned and operated by Arnout Hannink

    in close cooperation with
    - *Cozmanova,* owned and operated by Mark Dobrinic (www.cozmanova.com)
    - *SURFnet* 's RIES-team, including Xander Jansen and Jacques Schuurman (www.surfnet.nl)
    - *MS Insulinde*, owned and operated by Suze Maclaine Pont (www.msinsulinde.nl)
  - For more information, please contact
    - **Piet Maclaine Pont / MullPon**, Inventor of *DVBS* and *RIES* architect
    - Lynbaen 9
    - 8563 AZ Wijckel
    - The Netherlands
    - Web: www.mullpon.com
    - **E-mail: pietpont@mullpon.com**
    - GSM: +31 (0)641 267 617; Fax: +31 (0)514 605 945