

ISSS SIG proposal

Suisse-ID – benefits and risks for e-Commerce

Anthony Thorn

Background

Suisse-ID has received a lot of press coverage lately - at least compared to other IT-security topics. I am concerned that readers may get the impression that Suisse-ID solves all the problems of e-commerce security.

Suisse-ID brings clear security benefits, but the principal threat to e-commerce namely the compromise of the platform -operating system, browser or application- is not addressed.

The consequences of using a qualified personal certificate (such as Suisse-ID) on a compromised computer could be very serious indeed. There is no case law concerning the legal issues involved. The problem with PKIs for authenticating the general public is economic; namely that the merchant (or application service provider) reaps the benefit but the customer bears the costs – and not only the direct financial cost.

Task

I propose a new ISSS Special Interest Group (SIG, formerly known as Arbeitsgruppe) to address these issues. The language of the group will be German unless otherwise agreed. For additional information, refer to: <http://www.iss.ch/aktivitaeten/special-interest-groups/spielregeln/> .

My idea is to produce a detailed risk analysis for a generic e-commerce solution. This would show which countermeasures are effective against which threats. I think that an authoritative risk analysis would be a useful starting point for many organisations. Generic means as broad a range of types of e-transaction as possible, including web-shops and e-Banking, perhaps even e-Government if there is enough interest.

In addition we need to produce an equally authoritative summary for "lay-persons" which addresses security from the point of view of the e-Commerce customer.

Language:

Mix of English and German.

Kick-Off Meeting

The above title and description of the deliverables is preliminary and will be amended and agreed by those attending the kick-off meeting. The attendees will also agree scope, milestones, a timetable, and organisational issues.

Please reply by 27th May to: anthony.thorn@isss.ch if you want to work on this project. Provided there is sufficient interest you will receive an invitation to the kick-off meeting. You are welcome to contact me with questions or to propose improvements.

I hope to attract participants with practical experience of operating an e-commerce application as well as security and PKI experts. I would be grateful for offers of meeting rooms, preferably accessible with public transport.