Institute of Computer Science, University of Bern
Cryptographic Protocols, FS 2021

Prof. Christian Cachin
Jovana Mićić

Exercise 3

3.1 Privacy in the Google-One-VPN (10pt)

Google recently started to offer a (paid) VPN service (`https://one.google.com/about/vpn`). Operating a VPN service involves a tradeoff between the security of user authentication on the one hand, because only paying users should be able to use the VPN gateway, and privacy on the other hand, because the gateway operator should not learn the association between its users and the Internet addresses they access through the VPN.

Google resolved this tradeoff with blind RSA digital signatures ("advanced built-in security"); they ensure technically that Google *cannot* learn the association between users and Internet addresses in the VPN service.

This is a (rare?) example of the company respecting the principle of *privacy by design*: privacy is embedded into the architecture, privacy is the default, and user data is not collected if not necessary.

Google's white paper (`https://goo.gle/vpn-whitepaper`) describes the approach at a high level. The white paper is available in ILIAS with some annotations.

The task of this exercise is to understand the approach and to expand the design in the white paper. Starting with Figure 3, draw the architecture again, fill in details, and describe the protocol steps. You should include at least:

- Keys and cryptographic operations of the blind RSA digital signature scheme;
- User authentication, e.g., steps that involve the *Google userID* and checking whether the user has paid for the VPN service;
- Steps by the Key-Management Service within the *Data Tunnel Server (DTS)* when it receives the "unblinded signed token" and generates a *Data Tunnel Key (DTK)*;
- Steps by the VPN Client and the DTS to send and receive encrypted tunnel traffic.

In addition, explain the scope and lifetime of the RSA public/private key pair and the scope and lifetime of the DTK. (Notice that the document mentions at one point "a limited period of time.")