HIN access gateway commissioning (checklist)

This checklist includes all activities that need to be performed to ensure successful commissioning of the HIN access gateway.

[ ] Requirements for the integration of the HIN access gateway

In order for the access gateway (AGW) to perform the single sign-on, it checks the user against the active directory. The AGW is able to communicate with the active directory as follows:

- LDAP TLS or LDAPS
- NTLM or Kerberos

Requirements to be taken into account:

- Fixed public IP or fixed public IP range of client and AGW
- Internal URL with DNS resolution to hostname of AGW
- AD server (on-prem; from 2016) (currently only one domain is supported)
- AD server with SSL certificate (manual AGW, chapter 5.1)
- SSL certificate for AGW (from a CA known to the browser) (manual AGW, chapter 4.5)
- Firewall ports according to list (manual AGW, chapter 3.3.2)
- If Kerberos is being used; LDAP is read-only by user (manual AGW, chapter 5.2 ff)
- Email address for notifications (update notification) (manual AGW, chapter 4.4.7)
- Configuration of client browser by GPO (manual AGW, chapter 6)

[ ] Dimensioning of the HIN access gateway appliance

Dimensioning		The following resources are required for a virtual appliance:
[ ]	**Memory**	2 GB
[ ]	**Disk space**	5 GB
[ ]	**CPU**	1 virtual CPU

[ ] Use of the HIN access gateway as a virtual appliance

Type		Characteristics	Advantages
[ ]	**Virtual appliance**	Virtual appliance based on Linux, usable with VMWare ESX and Microsoft Hyper-V	Use of the available virtualized infrastructure (resources, redundancies, monitoring, etc.)

[ ]	**DNS entry**		
	For registration via the HIN access gateway, an internal DNS entry is required, which is also stated during the registration in HIN (auth URL). – It must be possible for the client located in your LAN to resolve this. If you use Kerberos, we recommend that the AGW hostname and the DNS entry are the same.		
	AGW VM	**DNS record**	**Value**

If you have an internal domain name with .local, please read point in the manual carefully.

Supported:

- 1 AD (with following methods: LDAP / LDAPS, NTLM or Kerberos)
- Mapping OU/AD groups to a specific AGW ID or team IDs, please refer to the manual for this.
- Users can link the HIN eID to their personal AD account. (Existing users who use the HIN client must have activated the SMS access (“SMS code”) in the service center).

[ ]	**Activating ports in the firewall and in the router**				
		Port	**Source**	**Destination**	**Description**
	[ ]	TCP 443 (https)	HIN access gate-way(s)	gateway2.hin.ch app.hin.ch auth.hin.ch agw-manager.hin.ch	Connection to the HIN data center for appli-cation access.
	[ ]	TCP 443 (https)	Clients (end users)	HIN access gateway(s)	Access to the access gateway for authenti-cation
	[ ]	TCP 389 (LDAP)	HIN access gate-way(s)	HIN access gateway(s)	Verification of the AD login
	[ ]	TCP 636 (LDAPS)	HIN access gate-way(s)	Active directory	Verification of the AD login
	[ ]	**TCP 88 (Ker-beros)**	HIN access gate-way(s)	Active directory	Verification of the Ker-beros token
	[ ]	TCP 2222 (ssh)	HIN access gate-way(s)	update2.agw.hin.ch	Connection to the HIN data center for the support connection
	[ ]	TCP 80 (http)	HIN access gate-way(s)	update2.agw.hin.ch	Obtaining system up-dates
	[ ]	TCP 4433	Admin clients	HIN access gateway(s)	HIN AGW Adminport
	Cluster: Activating ports if the AGW is being run in a cluster				
	[ ]	TCP 22 (ssh)	Between all cluster nodes		Required for the syn-chronization of the cluster settings
	[ ]	UDP 5404 - 5406	Between all cluster nodes		Required for switching virtual IP address

[ ]	**Network parameters for HIN access gateway**		
	[ ]	**Internal IP address for HIN access gateway appliance**	
	[ ]	**Subnet**	
	[ ]	**Host name for HIN access gateway**	
	[ ]	**IP address for default/standard gateway**	
	[ ]	**IP address for DNS server 1**	
	[ ]	**IP address for DNS server 2**	
	[ ]	**DC 1 and DC 2**	
	[ ]	**External IP address range(s) in which the clients and the HIN access gateway appliance are located (visible for HIN)**	

[ ]	**Cluster configuration**		
	The availability of the HIN access gateway can be increased by means of clustering.		
	[ ]	**No cluster**	
	[ ]	**Cluster**	
		Physical IP addresses	
		[ ] **Internal IP address of the second HIN access gateway**	
		[ ] **External IP address of the second HIN access gateway**	
		Virtual IP addresses	
		[ ] **Shared virtual IP address for both HIN access gateway instances** The AGW DNS entry is the same as the virtual IP.	

[ ]	**Coordination with HIN**	
	[ ]	**Agreement on the go-live date with HIN support** The go-live involves a test stage of one hour. During this time, the access gateway is registered and access to the HIN participant directory is tested in order to check whether commissioning of the HIN access gateway was successful. To do this, a date needs to be agreed with the HIN Integration Manager.

[ ]	**Clarification of the operating tasks**		
	[ ]	**Clarification of the operational tasks and responsibilities**	
	[ ]	**Technical operation**	
		[ ] **Scheduling of periodic backups**	
		[ ] **Scheduling the setting up of monitoring/integration in the monitoring infrastructure**	
		[ ] **Organization of the regular verification of logfiles**	
		[ ] **Organization of regular updates (notification email)**	
	[ ]	**Organizing support for internal users (technical/specialist)**	