

Start

if ( Log Counter == 0 )  
do Enclave-initialisation  
else  
skip

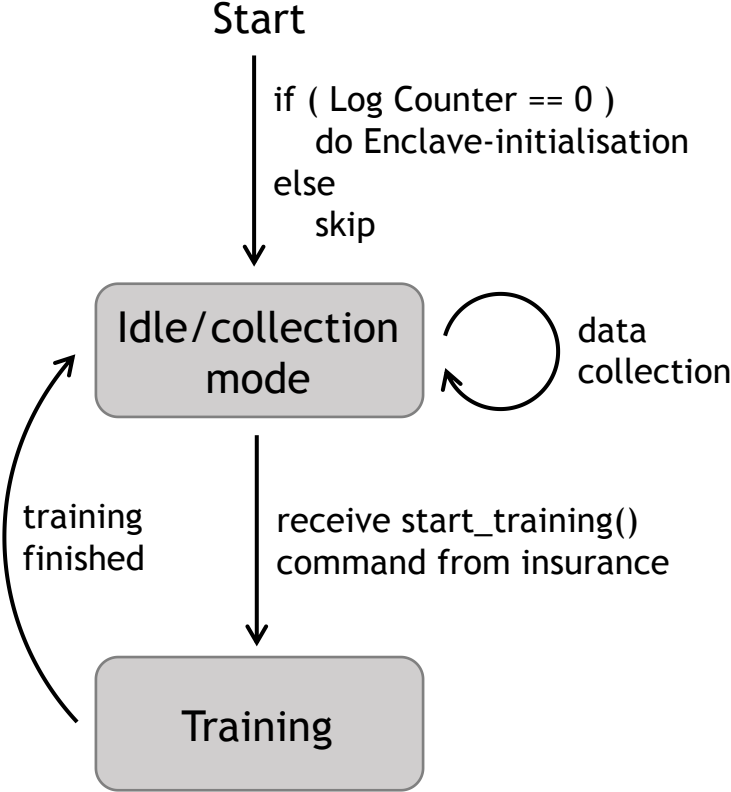
Idle/collection  
mode

data  
collection

training  
finished

receive start\_training()  
command from insurance

Training



# Enclave-initialisation:

## DP-GBDT Enclave

1b.  $c_{\log} \coloneqq \text{Read}()$

2. randomly choose master seed  $s_m$

3.  $\text{Log}_{\text{init}} \coloneqq \text{seal}(\{\text{"Log"}, \text{id}_{\text{LC}}, c_{\log}, s_m\})$

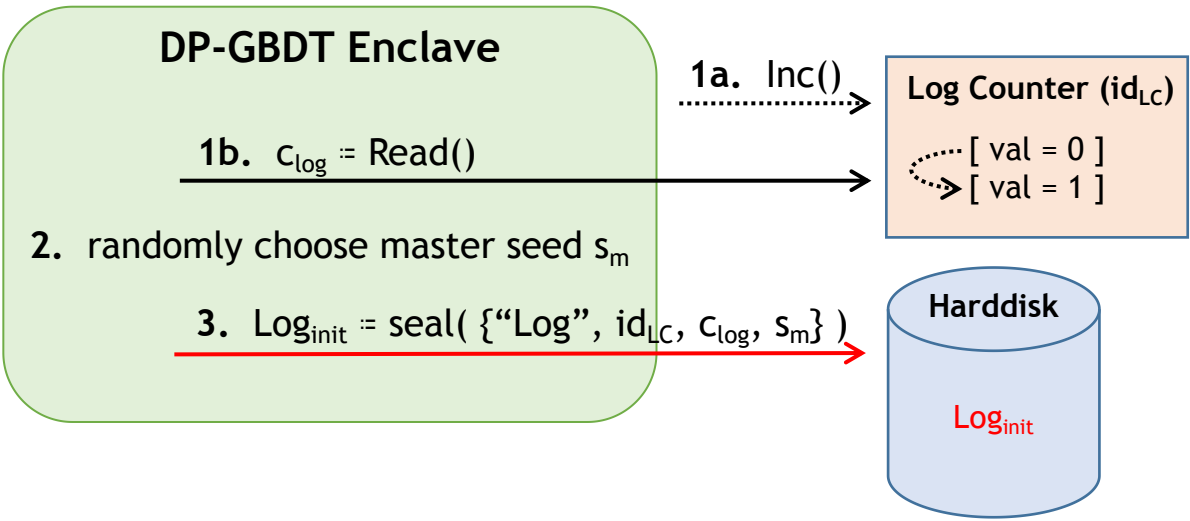
1a.  $\text{Inc}()$

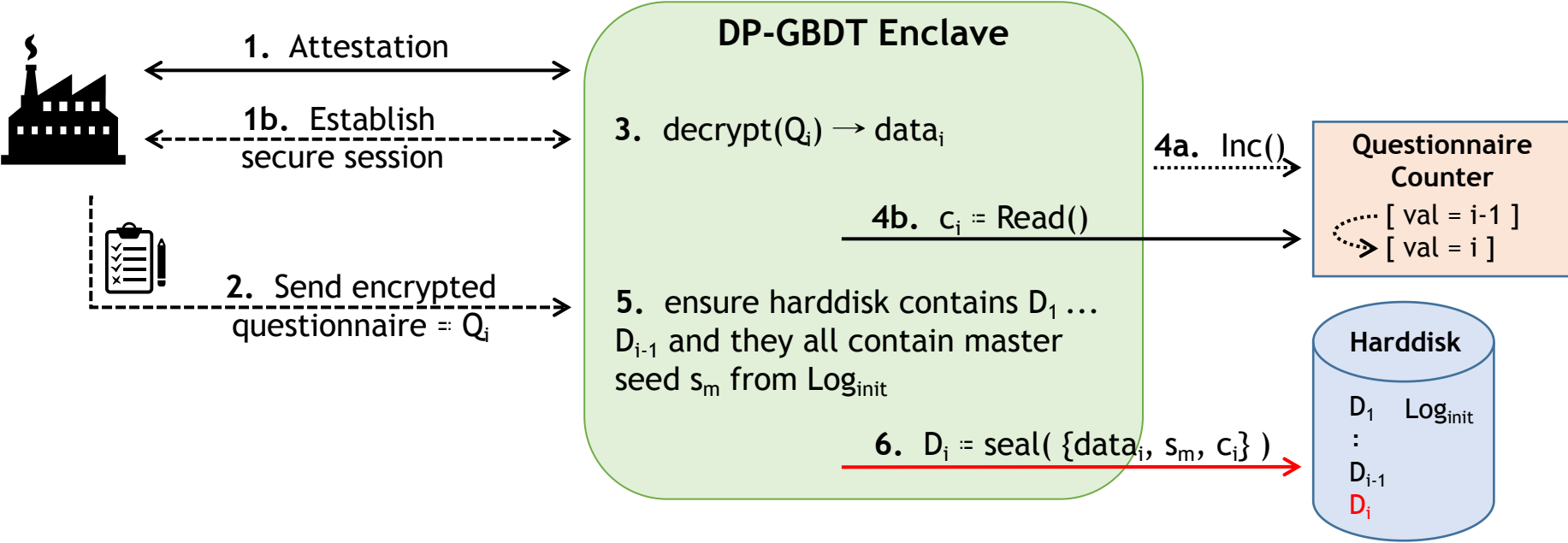
Log Counter ( $\text{id}_{\text{LC}}$ )

$\begin{matrix} \text{dotted arrow} & [ \text{val} = 0 ] \\ & \text{solid arrow} & [ \text{val} = 1 ] \end{matrix}$

Harddisk

$\text{Log}_{\text{init}}$

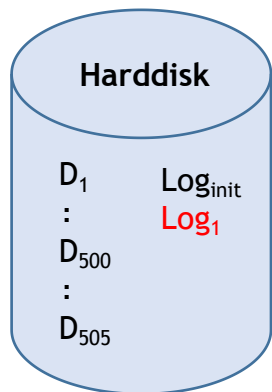






ZURICH<sup>®</sup>

1. train( $n = 500$ )



3a. load\*  $\text{Log}_{\text{init}}$  and  
 $D_1 \dots D_{500}$  into enclave

## DP-GBDT Enclave

2a. ensure  $n$  is valid training size

2b.  $c_q := \text{Read}()$

2c. ensure  $c_q \geq n$

4. (prng-)derive  $s_1$  from  $s_m$

5a. Inc()

5b.  $c_{\text{log}} := \text{Read}()$

6.  $\text{Log}_1 := \text{seal}(\{ \text{"Log"}, \text{id}_{\text{LC}}, c_{\text{log}}, 1, 500, s_1 \})$

7. start\_training( $D_1 \dots D_{500}, s_1$ )


8. output model

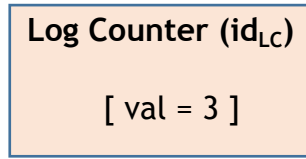
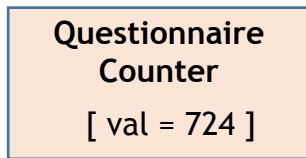
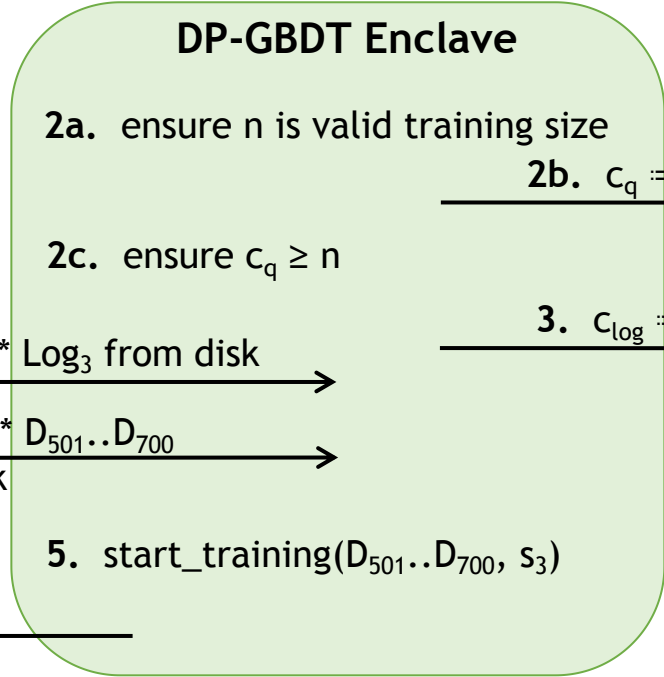
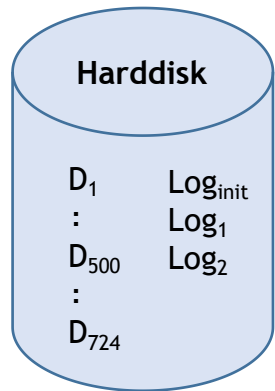
Questionnaire  
Counter

[ val = 505 ]

Log Counter ( $\text{id}_{\text{LC}}$ )

[ val = 1 ]  
[ val = 2 ]

 **ZURICH**  $\xrightarrow{1. \text{ train}(n = 700)}$



$\xrightarrow{6. \text{ output model}}$

**ZURICH** 1. train( $n = 700$ )

## DP-GBDT Enclave

2a. ensure  $n$  is valid training size

2b.  $c_q := \text{Read}()$

2c. ensure  $c_q \geq n$

Questionnaire  
Counter

[ val = 724 ]

3.  $c_{\log} := \text{Read}() = 2$

5a. Inc()

Log Counter ( $\text{id}_{\text{LC}}$ )

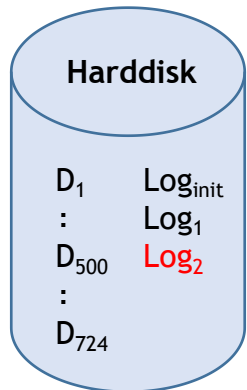
[ val = 2 ]  
→ [ val = 3 ]

5b.  $c_{\log} := \text{Read}() = 3$

6. (prng-)derive  $s_2$  from  $s_m$

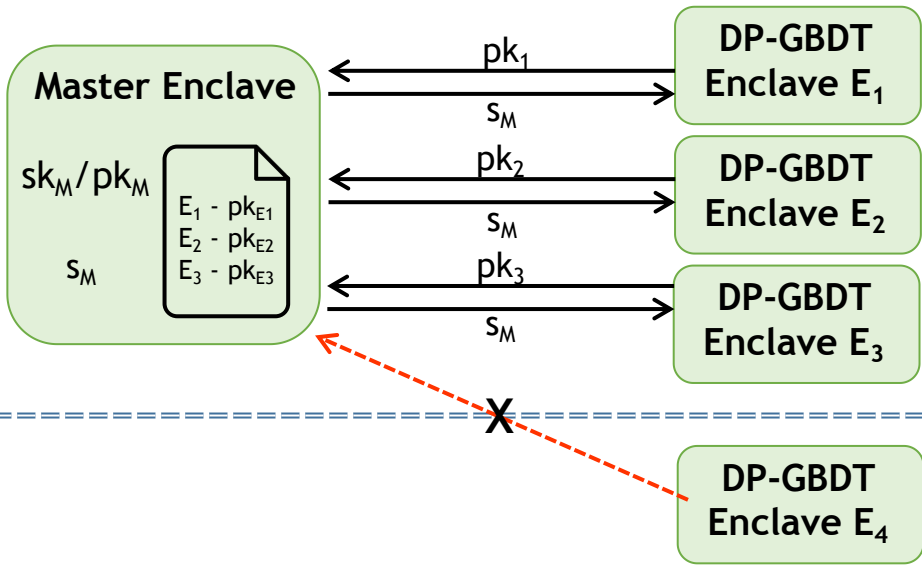
7.  $\text{Log}_2 := \text{seal}(\{ \text{"Log"}, \text{id}_{\text{LC}}, c_{\log}, 501, 700, s_m, s_2 \})$

8. start\_training( $D_{501} \dots D_{700}, s_2$ )



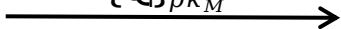
4. load\*  $\text{Log}_{\text{init}}$  and  
 $D_{501} \dots D_{700}$  into enclave

9. output model



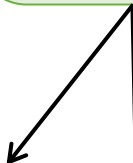
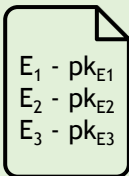


$\{Q_i\}_{pk_M}$



**Master Enclave**

$sk_M/pk_M$



$\{Q_i\}_{pk_{Ej}}$

**DP-GRDT  
Enclave E1**

$sk_{E1}/pk_{E1}$



**DP-GRDT  
Enclave E2**

$sk_{E2}/pk_{E2}$

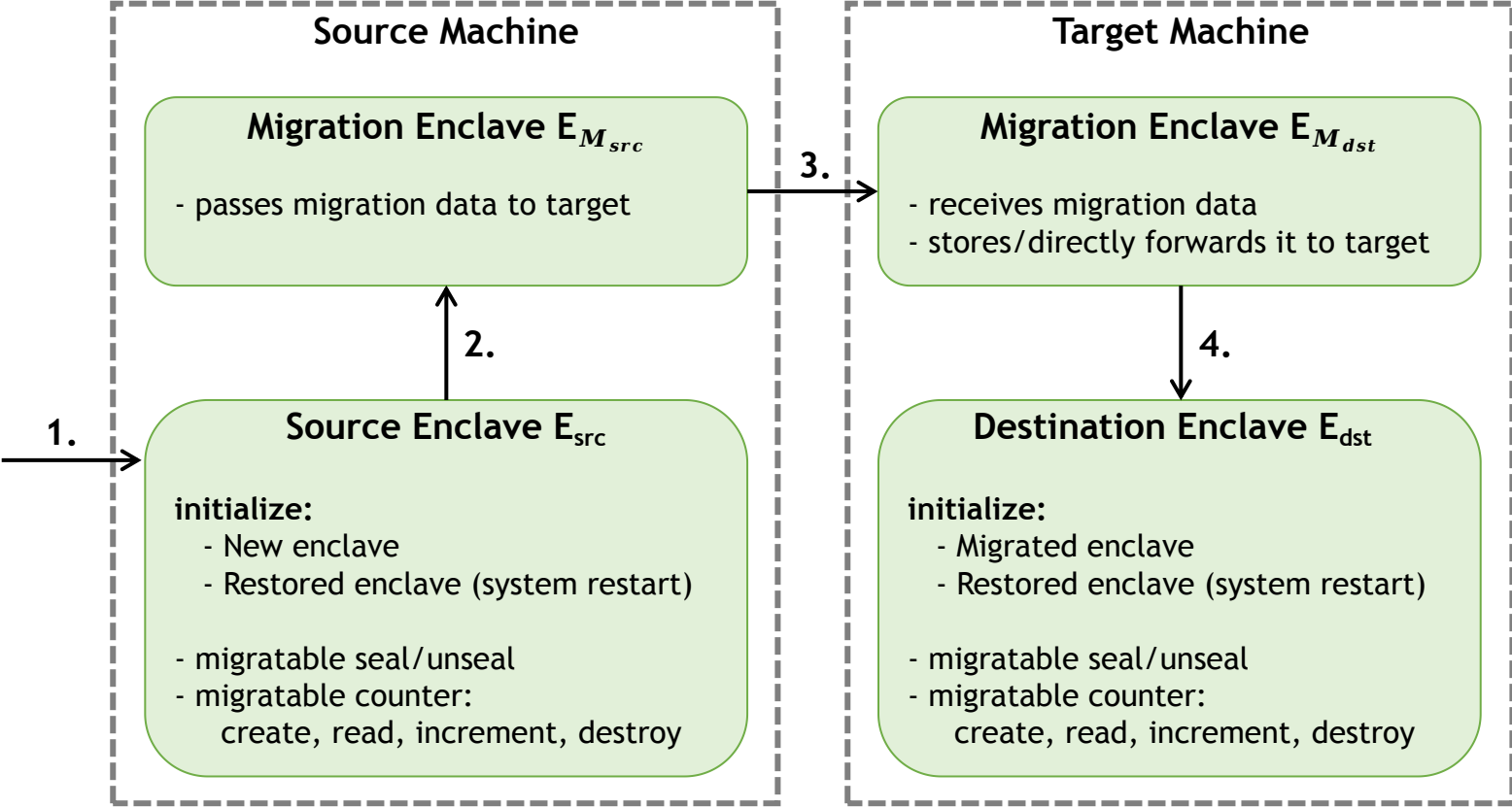


**DP-GRDT  
Enclave E3**

$sk_{E3}/pk_{E3}$







cpp\_gbdt

python\_gbdt

hardened\_gbdt

enclave\_gbdt

hardened\_  
enclave\_gbdt

