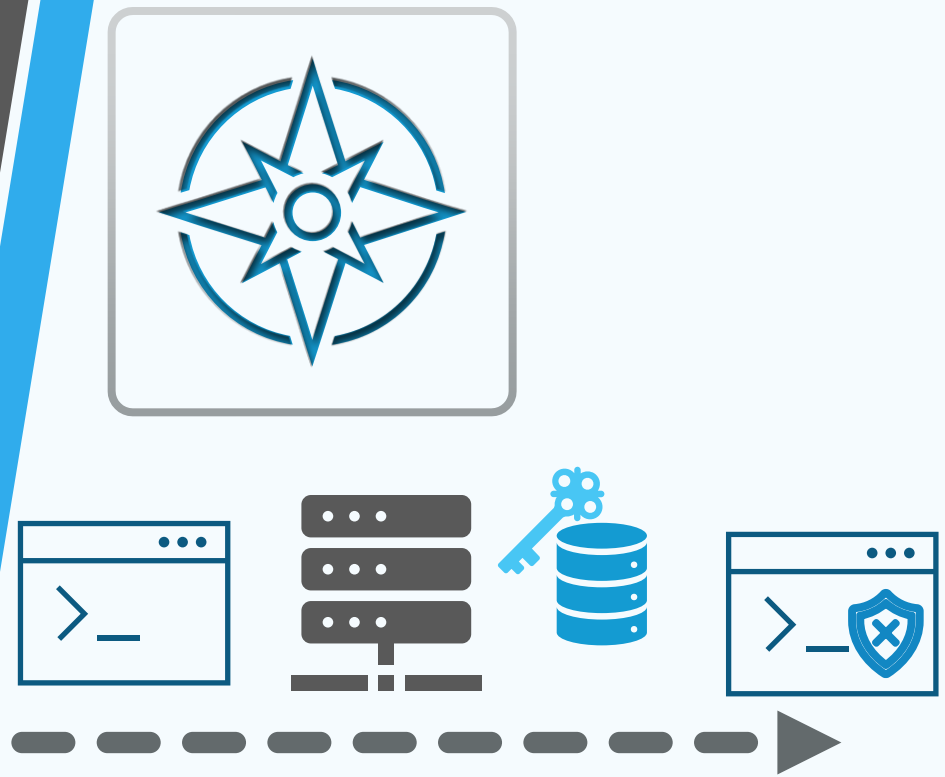
ATTESTING WHAT AND HOW.

NOVEL FORMS OF ATTESTATIONS.

PROLOGUE I



- FRENCH SME
- OUR MOTIVATION: NEW CYBER SECURITY METHODS
- OUR WAY: EXECUTABLE REWRITING THROUGH SECAAS
- DIFFERENT THREATS COVERED (INTEGRITY, CONFIDENTIALITY, CLONING, SUPPLY CHAIN)
- OUR PROPELLER: CODE BASIS + SEVERAL COLLABORATIVE PROJETS
- OUR BEARING: AUTOMATIC ALWAYS SUSTAINABLE SECURITY

PROLOGUE II. ATTESTATION BACKGROUND

REMOTE ATTESTATION:

- AT LEAST A 3-PARTY COMEDY: THE MEASURED, THE ATTESTOR AND THE VERIFYER.
- PROOF OF DENTITY AND ORIGIN OF A PIECE OF CODE OR SYSTEM STACK
- LOAD TIME AND SYSTEM VERIFICATION BEFORE USE
- IMPLICIT OR EXPLICIT ATTESTATION

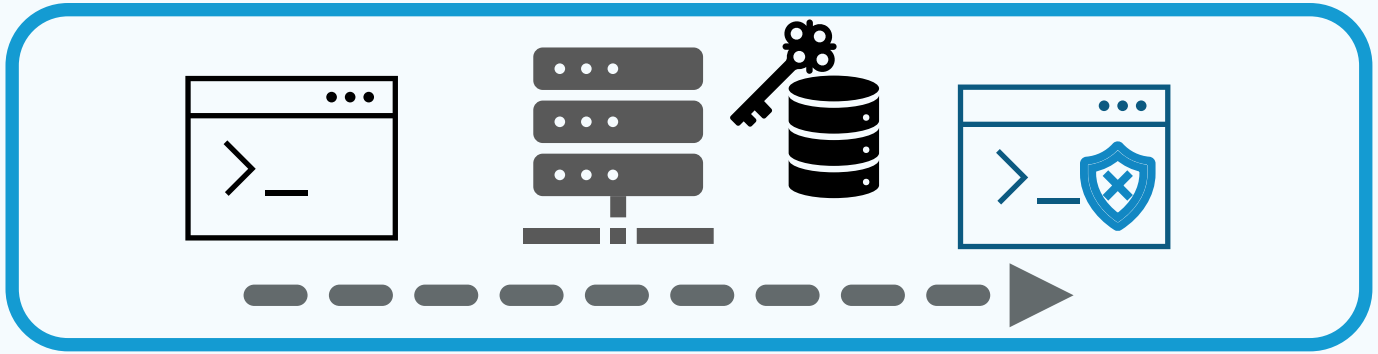
SECURITY:

- **SECURE** VERIFIER AND REFERENCE MEASUREMENT STORE: AT AN A PRIORI TRUSTED LOCATION
- **IN THE WILD EXPOSED** ATTESTERS, SECURED BY TCB TECHNIQUES (EG, TEE, TPM)
- EXCHANGES SECURED BY PROTOCOLS

OPERATIONAL PAIN POINTS:

- REFERENCE MEASUREMENTS TIMELY DISTRIBUTION
- SYSTEM OR INFRA SOFTWARE REQS (EG, VERIFIER SERVER, TPM, KERNEL MODULE)
- LATENCY

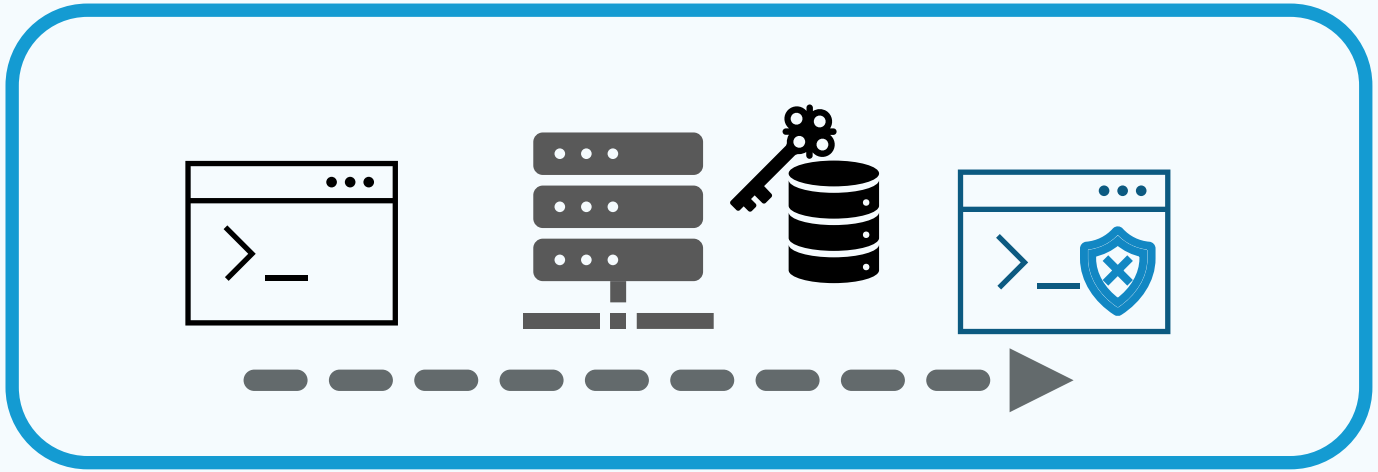
MOTIVATIONS



DI
P

PAIN POINTS - PITFALL REMOVAL.
NOVEL SCHEMES.
NOVEL ENDORSEMENTS

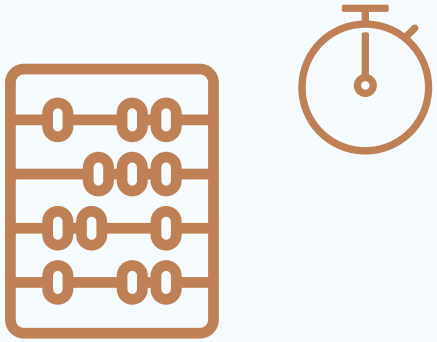
PAIN KILLER



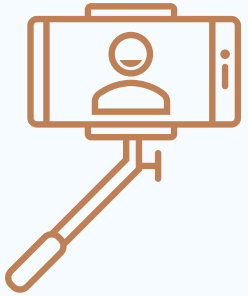
MANIFESTS PRODUCED AT SECAAS

RIDE-ON EXECUTABLES
(Incl V&A PRIMITIVES, MANIFESTS, Pub Key)

BACKGROUND ON ATTESTATION (1)



SENDATE TANDEM



EMBEDDED SELF-AUTHENTICATION

INSIDE OUR PACKAGED SW X-SECURITY HARDENINGS (INT/CONF)

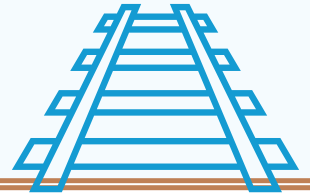
AUTH OBJECTS: EXECUTABLES AND LIBRAIRIES

FIRST ACTION TAKEN BEFORE UNPACKING OR LIB CALL

TRUSTWOTHINESS  ATTESTOR AND VERIFIER

BACKGROUND ON ATTESTATION (2)

INSPIRE-5Gplus



SENDATE TANDEM

CONTROL FLOW SIGNALING EXTRACTIONS. RUNTIME VALIDATION

INTEL SGX IMPLEMENTATION

LIB FUNCTIONS AT CALLED TIME

HEARTBEATS (PROOF OF EXECUTION, FRESH INTEGRITY CHECK)

TRUSTWORTHINESS

ON GOING WORK ON ATTESTATION (1)

DESIRE6G

INSPIRE-5Gplus

DLT-POWERED **MUTUAL** ATTESTATION (CHAIN OF TRUST)

RUNTIME ATTESTATIONS:

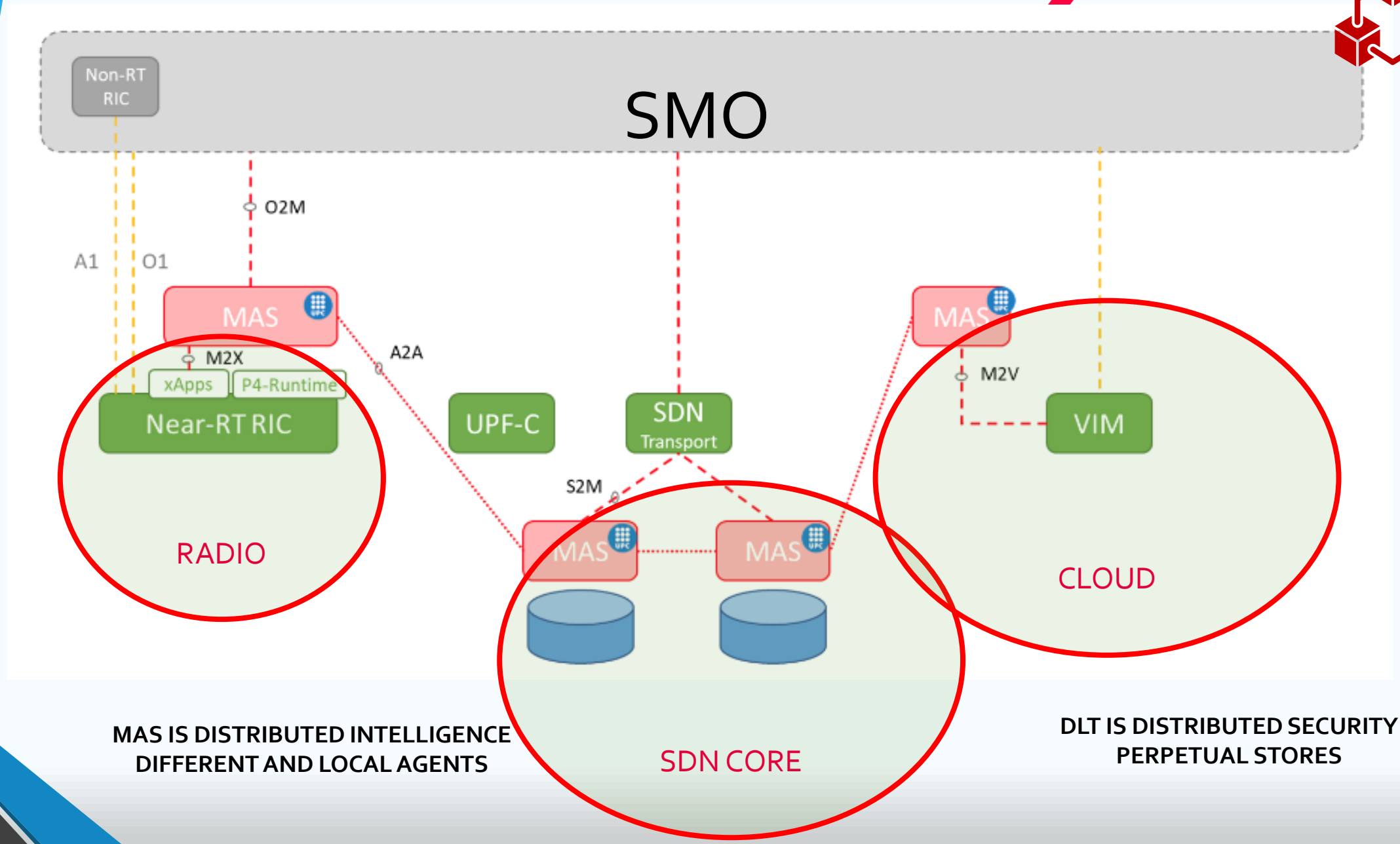
PROOF OF EFFECTIVE EXECUTION

PROOF OF NORMAL EXECUTION

TRUSTWORTHINESS BASED SW CHAIN OF TRUST

DISTRIBUTED SECURITY BY DLT

ON GOING WORK ON ATTESTATION (2)



MAS IS DISTRIBUTED INTELLIGENCE DIFFERENT AND LOCAL AGENTS

DLT IS DISTRIBUTED SECURITY PERPETUAL STORES

DLT-POWERED MUTUAL ATTESTATION

DESIRE6G

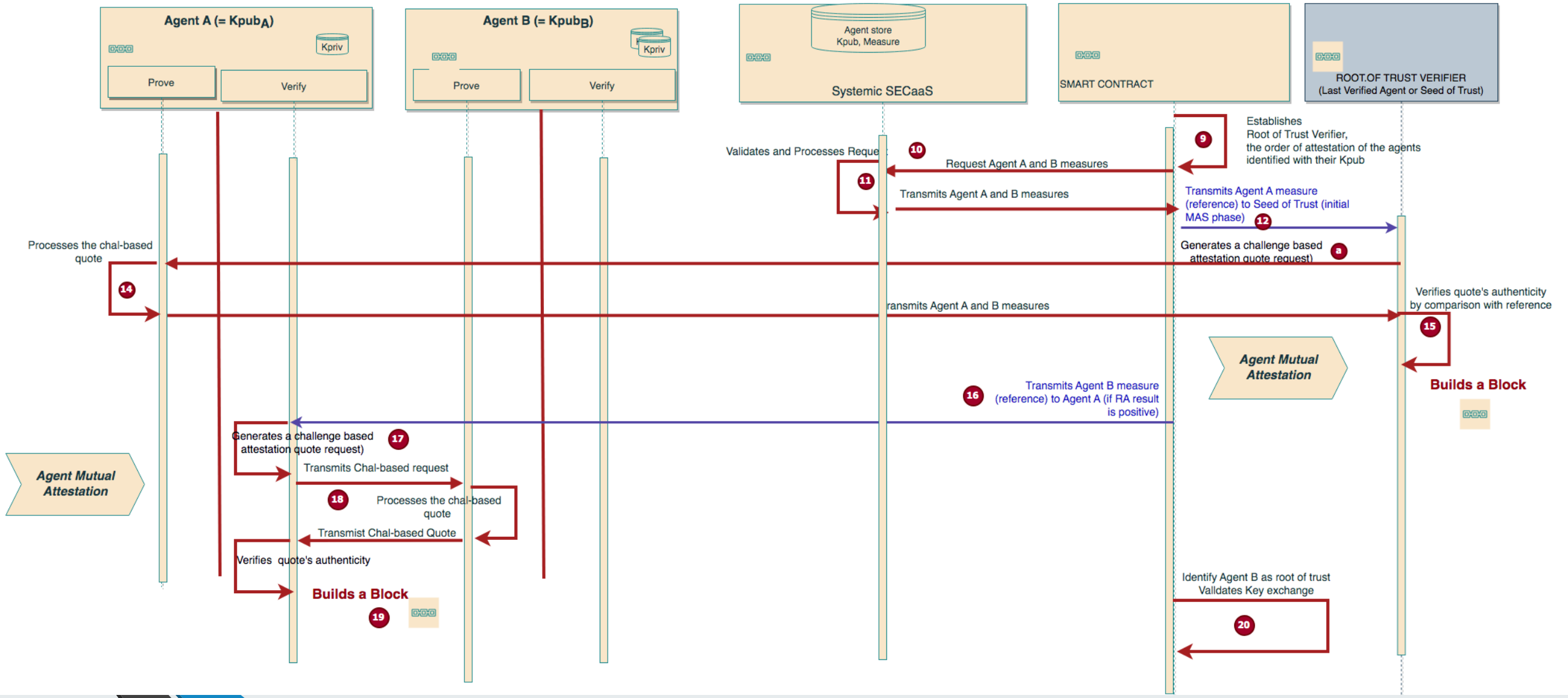
SOLUTION FEATURES

- CHAIN OF TRUST: FRESHLY ATTESTED AGENTS ARE ELECTED VERIFIERS (SMART CONTRACT)
- SMART CONTRACT ORCHESTRATE RA JOBS AND DISTRIBUTES MANIFESTS TO ELECTED VERIFIERS
- BLOCKS ARE PRODUCED BY ELECTED AGENTS AND CONTAINS RA RESULTS

EVOLUTION

- AGENT CONTINOUS TRUST, BASED ON RUNTIME COLLECTED METADATA

MUTUAL ATTESTATION SEQUENCE DIAGRAM

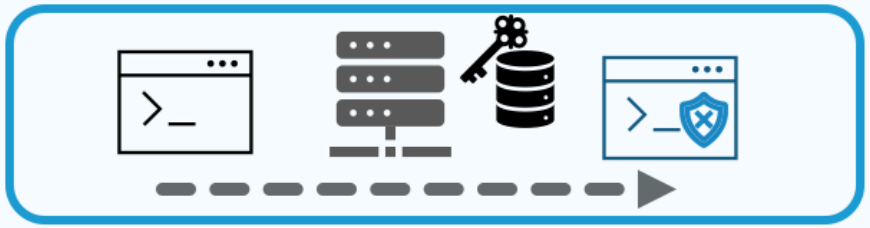


NOVEL ENDORSEMENTS.

SLAS TELL OR ENSURE THAT THE SW IS INTEGRATED, TRULLY RUNS AT A GIVEN TIME, RUNS AT THE CORRECT PACE, RUNS AT THE CORRECT LOCATION, RUNS INSIDE A TEE OR AN ISOLATED MEMORY COMPARTMENT, IS SURROUNDED BY AFFINITY-COMPLIANT PROCESSES, CAN BE IDENTIFIED (WITH DIFFERENT GRANULARITY), CONTAINS CERTIFICATES OF QUALITY AND SECURITY RELATED PRACTICES AT BUILD TIME, IS ENABLED WITH USER RIGHT ENFORCEMENT.

- AUTHENTICATION
- RUNTIME INTEGRITY
- EFFECTIVE EXECUTION
- PERFORMANCE RATIO
- LOCALITY ENFORCEMENT
- TEE EXECUTION / MEMORY COMPARTMENTALIZATION
- SURROUNDING PROCESSES IDENTIFICATION
- IDENTIFICATION (EG, VERSION, SINGULAR ARTIFACTS, BY WATERMARK)
- CONTAINS QUALITY ASSURANCE-RELATED CERTIFIED STAMPS
- CONTAINS SECURITY RELATED STAMPS
- DIGITAL RIGHT MANAGEMENT TEST

EPILOGUE. CONCLUSIONS



APPLICATION SOFTWARE
RIDE ON, AUTONOMOUS
CROSS-DOMAIN TRAVERSAL
SEVERAL TRUSTWORTHINESS LEVELS
DECENTRALIZED VERIFICATION BY DLT
NEW ENDORSEMENTS