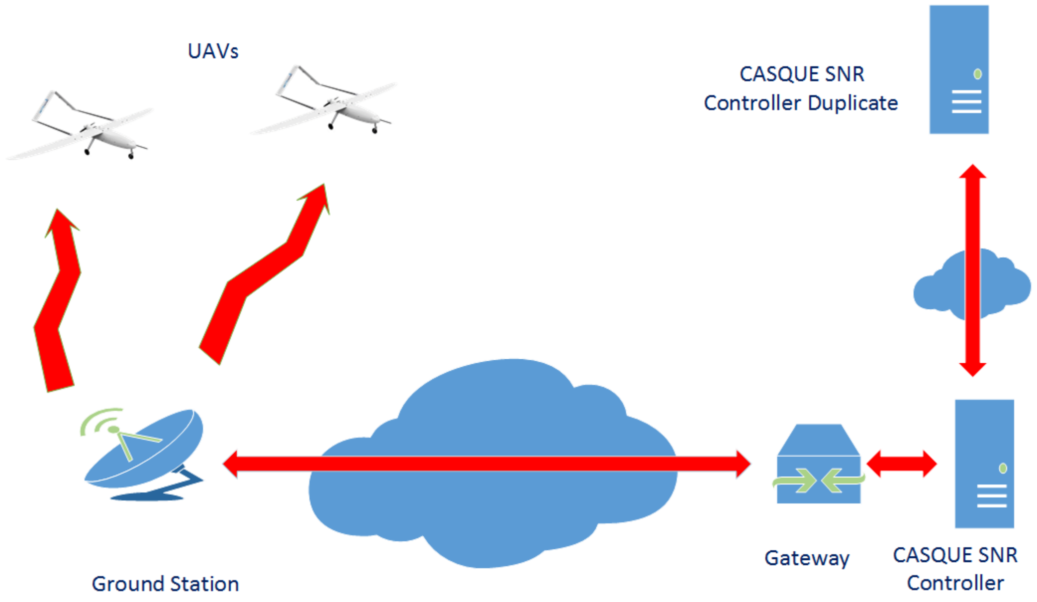
CASQUE SNR for Internet of Things

[1] Application Functionality

In order to propose a generic solution to the safety of communications in the setting of the Internet of Things it is useful to examine a few real application requirements. The benefits of considering a solution which has more universal applicability is that the constraints of a given solution are better exposed and that the resulting design has greater flexibility.

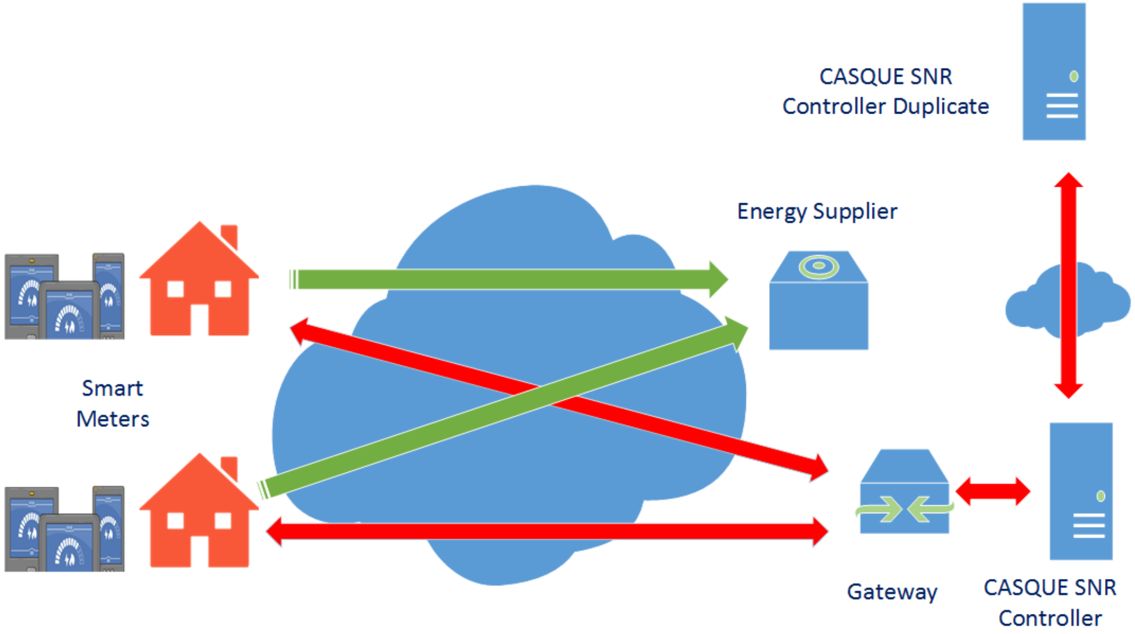
[1.1] UAV Example



This requirement is the target of a current Research Contract that Distributed Management Systems have recently been awarded by UK’s NATEP. The desired solution is to retrofit existing Ground Station and child UAVs so that each party can authenticate each other and then set up end to end encrypted communications. Man-in-the-Middle attacks must be prevented.

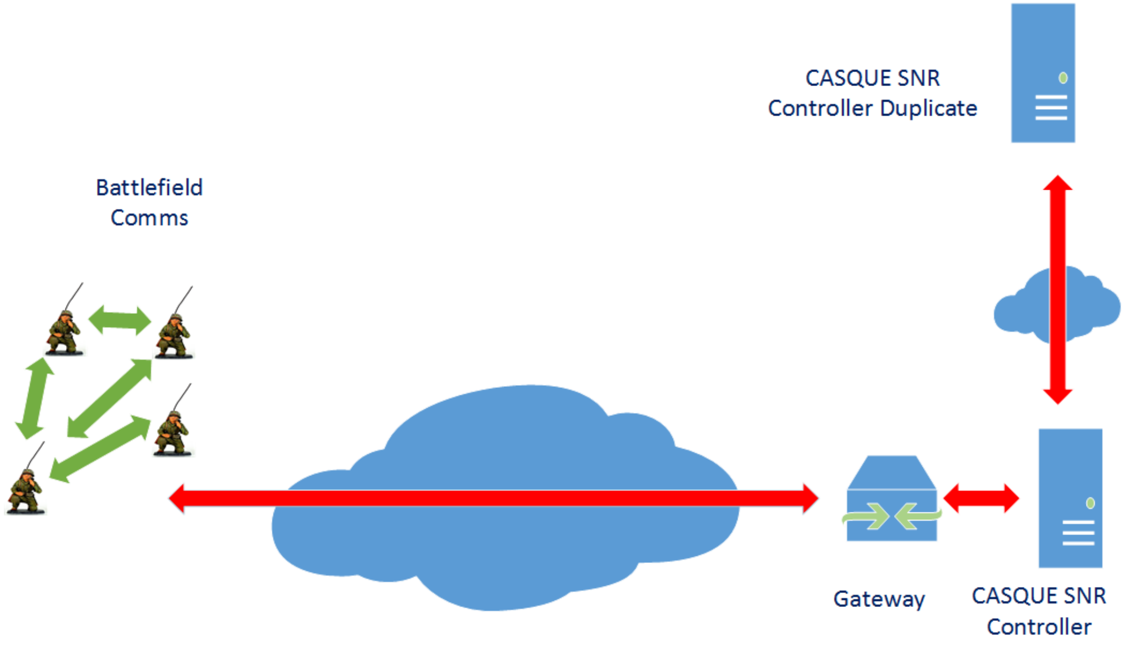
Deployment contingencies mean that connection to the Central Servers cannot be assumed but a preparatory phase is always allowed so that the flight can be prepared with access to central Servers. This means that the encryption keys need to reside in each of the participating parties albeit with limited validity time periods.

[1.2] Smart Meters



The communication needs to be safe between the Home and the collecting and monitoring Server usually sited at the Energy Provider. Man-in-the Middle attacks must be denied. The issue of performance is relevant as the number of homes serviced is usually very large- i.e. many millions. The requirement to easily recover from Denial of Service attacks is important.

[2.3] Battlefield Communications



Here the requirement is to have a group of Soldiers being able to mutually authenticate and to communicate safely with each other. Man-in-the Middle attacks must be denied. The Central Servers may not be available in the deployment phase.

[2] High Level Design

[2.1] Identities

The core of the system to enable secure communications is the secure element of the CASQUE SNR Token which is based on an EAL5+ rated Smartcard/SIM. Once populated by CASQUE SNR's SAS system each Smartcard has an identity. It is clear from the examples quoted above that each party may only have a restricted number of other parties with which there is a need to communicate. It is assumed that either a human administrator sets up this profile on each party or alternatively the Central Server imposes on each party their dialogue mates. The latter option is more complicated to implement.

[2.2] Computing Resources

It is assumed that each party has sufficient computing power to execute the common Internet protocols, has a fixed IP address and also the means to execute the common cryptographic algorithms and the means to communicate with the CASQUE SNR Smartcard/Sim using PC/SC AT commands. Typically this will be a local hub to which less intelligent sensors are attached.

[2.3] Party to Party Communication Request

In the case when a party knows the CASQUE SNR Identity of the target party then such a request can be made to the CASQUE SNR Authentication Server. There then follows an exchange, by each side, of random encrypted with one of the client party's static encryption keys. The composite random is then the session encryption key.

Once this secure link is established a normal Challenge Message is sent by the Authentication Server (which may involve a Key Change) in order to authenticate the client party. If the request is granted, the Authentication Server returns two versions of the session key identifier, session key and its expiry date – one encrypted by one of the requestor's keys and the other encrypted by one of the target's keys.

The client party then sends this data, called the Communication Keyset (CK), to the target party. Both parties can now both exchange their own random encrypted with the session key to form the actual session key to be used in the subsequent communication.

The CRE is locally stored by each party but the ephemeral session key generated by this key is not stored so forward secrecy is maintained. On subsequent communications between the same two parties just the session key identifier needs to be sent assuming the expiry date is not exceeded.

[2.4] Sending Communication Request Enabler (CRE)

The sending of the CRE can be formalised using JOSE – JSON Object Signing and Encryption. This technique facilitates the use of this system when the underlying Op Systems of Parties are different.

[3] Security Target

[3.1] Security Assurance Criteria (SAC)

The Electronic Frontier Foundation’s Scorecard (https://www.eff.org/secure-messaging-scorecard) has listed some useful tests on how to rate a particular secure messaging system. The answers below show how the proposed scheme fulfils the recommended functionality.

EEF SAC 1. Is your communication encrypted in transit?

Yes

EEF SAC 2. Is your communication encrypted with a key the provider doesn't have access to?

The actual session encryption key used is solely created by the two parties concerned and is not saved after the session ends. The CASQUE SNR Smartcard has keys populate by the customer with no involvement from the manufacturer (DMS) nor the System Integrator.

EEF SAC 3. Can you independently verify your correspondent's identity?

The client has to be authenticated by the Server before any request for communication can be made. The nature of the creation of the session key ensures both parties are mutually authenticated.

EEF SAC 4. Are past communications secure if your keys are stolen?

This criterion requires that the application provides forward secrecy, that is, all communications must be encrypted with ephemeral keys which are routinely deleted along with the random values used to derive them.

EEF SAC 5. Is the code open to independent review?

Yes and the core system CASQUE SNR has been certified at source code level by CESG, the UK National Authority for Information Assurance. Any customer can view the source code and there is available full source code Escrow for any Customer.

EEF SAC 6. Is the crypto design well-documented?

Yes

EEF SAC 7. Has there been an independent security audit?

Yes, The core functions of CASQUE SNR has been certified at source code level under CESG (the UK Government's National Technical Authority for Information Assurance) CAPS scheme and can be used for UK Government applications.

[3.2] Extended Assurance Criteria (DMS ESAC)

Whilst satisfying the above tests is clearly desirable it is not sufficient to obtain a “High Assurance” accolade as the following weak features can still remain. Most messaging protocols currently proposed suffer from some or all of the weaknesses defined below.

DMS ESAC 1 Does the security rely on a fixed secret?

Systems that depend on a Private Key in PKI or a defined global Authorisation Key are weak since the fixed secret maybe be passed on or found out, for example, by factorisation methods. In the case of a large deployment such vulnerability may prove catastrophic both in payload damage and recovery costs.

Keys in the CASQUE SNR secure element are routinely changed either on every interaction with the Authentication Server or periodically or by instigation from a System Administrator.

In fact, all the Keys in the secure element can be completely refreshed at a standalone admin system at the customer’s premises.

DMS ESAC 2 Can the design prevent Man-in-the-Middle Attacks?

Yes- there is no Public Key transferred in the CASQUE SNR dialogue so there can be no possibility of a Man-in-the-Middle Attack.

DMS ESAC 3 Does the Hardware Secure Element have independent review?

CASQUE SNR has a manifestation using Giesecke & Devrient EAL5+, FIPS 140-2 Level 3 rated Smartcard/SIm

DMS ESAC 4 Can a Privileged insider take a copy of the Server and predict keys?

Every key injected into the CASQUE SNR secure element at key change is created on the fly using external seeds and internal system dependent nonces that cannot be duplicated by Server copying.

DMS ESAC 5 Can the system clients operate without the continuous access to an Internet connected Central Server?

Yes