A. Counter Measure List

A.1. Technical Counter Measures

Some of the technical counter measures result in a Boolean value (i.e. the call is suspicious to Spam or the call is most likely to be legitimate), but others result in a real value, the Spam Feedback Value (calls with a high Spam Feedback Value are more likely to be spam). In order to make a decision the Spam Feedback Value is translated into a Boolean value by means of a threshold, which is set conform the required strictness of the system.

In this list the term ID is used for the ID of the user (e.g. telephone number, SIP URI, TEL URI, etc.)

White Listing	Maintain a list with IDs that are allowed to make a conversation with the callee (also called buddy list). All other IDs get a special treatment (e.g. blocking, redirecting to Turing Test, etc.). White Listing can be implemented by private lists or group lists. **Requirements**: Strong identity **Problems**: Introduction problem
Black Listing	Maintain a list with IDs that get a special treatment when making a conversation with the callee (e.g. blocking, redirecting to Turing Test, etc.). All other IDs are allowed to directly make a conversation with the callee. Black Listing can be implemented by private lists or group lists. **Requirements**: Strong identity, list management, it should be difficult to obtain a fresh identity **Problem**: Conversion of 'bad guys'
Gray Listing	Every caller gets a behaviour value, based on its behaviour in the past. This value is increasing in case of 'bad behaviour' and decreasing in case of 'good behaviour'. The Spam Feedback Value is equal to this behaviour value. **Requirements**: Strong identity **Problems**: to be defined
Turing Test	The caller, who tries to initiate a call with the callee, has to proof that he is a human being and not a machine by means of a test. This test should disclose whether or not the caller is able to do something that is difficult for a machine (e.g. voice recognition, human conversation pattern, entering welcome message). **Requirements:** A test for which it is hard to program a machine in such a way that it passes the test **Problem**: Could be difficult for disabled people, does not block Spam originating from call centres.
Callee Feedback	After a call is ended the callee has to decide whether or not it was Spam and he gives the feedback to the system. This feedback can be input for other counter measures. **Requirements**: Co-operation of the end-users, trust in the end-user **Problems**: to be defined
Content Analysis	During the conversation the content is analysed to establish the Spam Feedback Value. The content analysis can be done with Speech-to-Text tools or with human conversation pattern observation. **Requirements**: High computational power **Problems**: Not possible in case of end-to-end encryption. contradicts with personal privacy

IP/Domain Correlation	By observing the caller's ID, domain and IP address three suspicious situations can be identified: 1. Calls from different domain and from the same IP address 2. Calls from the same ID and from different IP addresses 3. Different callers from same domain and from the same IP address. Situation 1 should result in the highest Spam Feedback Value. Situation 2, which can be legitimate in case of a mobile device, should result in the second highest Spam Feedback Value. Situation 3, which can be legitimate in case of a NAT, should result in the third highest Spam Feedback Value. All other situations, which are not suspicious to Spam, should result in the lowest Spam Feedback Value possible. **Requirements**: to be defined **Problems**: High false positive rate
Domain of Trust	Every domain has a certain Trust Value in accordance with the likeliness of spam, which originates from this domain. The Trust Value is computed by means of some known security characteristics on that domain (e.g. possibilities for spoofing, possibilities for obtaining a new identity, effectiveness of the implemented Spam counter measures, etc.). This method can be implemented using a Central Authority which issues certificates to all domains. Low Trust Values result in a high Spam Feedback Value. **Requirements**: Trust in the issued certificates **Problems**: to be defined
Statistical Metrics / Signalling Protocol Analysis	Caller's behaviour can be analysed using statistical metrics (e.g. Number of simultaneous calls, call rates, spacing between calls, call duration). With these metrics some standard profile has to be defined according to legitimate behaviour. The Spam Feedback Value is linear with respect to the variation from this standard profile. **Requirement:** Strong identity **Problems**: False Positives
Progressive Multi Gray Levelling (PMG)	This is a special variant of Gray Listing. As a result of the observed call pattern, the caller gets a short term behaviour value, which is increasing/decreasing quickly, and a long term behaviour value, which is increasing/decreasing slower. The addition of these two values will result in the Spam Feedback Value. **Requirements**: Good method to observe the call pattern, strong identity **Problems**: to be defined
Reputation System / Web of Trust	In this approach every caller defines trust values for other callers and this will end up in a social network. Every time a caller wants to initiate a conversation with a callee the mean value of all shortest paths is calculated. **Requirements**: Co-operation of the end-user, trust in the end-user, strong identity **Problems**: to be defined
Honeypot	Some dedicated phone lines are configured to always answering and playing a pre-recorded message. The activity on such lines is monitored and can be result in information which is input for other counter measures (e.g. Black Listing). Random dialling will sooner or later end up on such a Honeypot. **Requirements**: to be defined **Problem**: Also human beings can accidentally end up on a Honey pot.
Multiple ID's	A user has a main ID, which he only gives to people he trust, and one or more other ID's, which he can use for communication with people he do not trust. These ID's then can have some limitations (e.g. only accessible within some time window, only accessible in a certain geographic region, only accessible from a certain trusted domain) **Requirements**: easy ID management for the user **Problems**: to be defined

A.2. Legal Counter Measures

Anti-Spam Legislation	Spam is punishable by law. If the punishment is heavy enough and the chance to be caught is high enough, this will discourage people to Spam. **Requirements**: Co-operation of the (worldwide) government **Problems**: Spam originates from mistrusted countries

A.3. Social Counter Measures

Immediately Contact Originator	When spamming behaviour is discovered, the originator is contacted immediately by the Network Operator and asked the question what he is doing. This could discourage the spammer even in an early stage. **Requirements**: Good method to detect Spam **Problems**: A legitimate user's computer is misused for Spam
Do Not React	Ignore negative behaviour and only react on positive behaviour. An advice for the user is to never buy anything offered via Spam. **Requirements**: Co-operation of all end-users **Problems**: to be defined

A.4. Commercial Counter Measures

No Free Calls	Every phone call costs a certain (small) amount of money. This way it is less attractive to use VoIP Spam for advertisements. **Requirements**: Strong identity **Problems**: to be defined
Payment at Risk	Every time when a call is established between the caller and the callee the caller immediately pays a certain (small) amount of money. Only if the user decides that the phone call was Spam the caller loses his money, otherwise he gets his money back. This way it is less attractive to use VoIP Spam for advertisements. The money must go to some non-profit organisation, otherwise this will become a business model. **Requirement**: Safe micro-payment system, trust in the end-user, strong identity **Problems**: to be defined